NASA Contractor Report 3488

A Tutorial on the CARE III Approach to Reliability Modeling

Kishor S. Trivedi and Robert M. Geist

GRANT NAG1-70
DECEMBER 1981

NASA

NASA Contractor Report 3488

A Tutorial on the CARE III Approach to Reliability Modeling

Kishor S. Trivedi and Robert M. Geist
Duke University
Durham, North Carolina

Prepared for
Langley Research Center
under Grant NAG1-70

National Aeronautics
and Space Administration

**Scientific and Technical
Information Branch**

1981

1.0 Introduction

The design of fault-tolerant avionics and control systems needs to be supported by an assessment of whether the systems possess the level of reliability for which they were designed. Because ultra-high reliability requirements exist for such systems, an experimental approach based on lifetesting techniques cannot be used to evaluate them [1,2]. Analytical models based on stochastic assumptions must then be developed to help predict and validate the reliability of these systems.

Early approaches to reliability prediction were based on a combinatorial method first discussed by Mathur and Avizienis [3]. Their method assumed that the system was a series of subsystems, each of which was to be modeled as a hybrid NMR type. The reconfiguration mechanism was assumed to be perfect. Bouricius and his colleagues extended this model to allow the reconfiguration mechanism to have an imperfect coverage [4]. As an embodiment of this notion, the CARE program was developed at JPL as a computer-aided reliability evaluation package. This was later modified by Raytheon and was named CARE II [5].

Not all systems of interest can be broken down into a series of smaller subsystems. In such cases, combinatorial methods have been superseded by more general Markov chain methods. Ng and Avizienis [6] have developed a unified model for the reliability evaluation of nonmaintained (closed) fault-tolerant systems based on a Markov approach. These ideas have been incorporated into a computer-based reliability evaluation package known as ARIES [7].

Several limitations of the early approaches became evident with their use in modeling ultra-reliable, fault-tolerant systems such as SIFT [8] and FTMP [9]. First, fault coverage was assumed to be a single number, whereas in practice, the times to detect, isolate, and recover from a fault are nonzero random variables. Furthermore, these quantities do depend on the current state of the system. The implication is that the fault-handling behavior of the system needs to be modeled and one or more parameters need to be derived capturing the coverage aspects. Such a coverage model is already a part of CARE II and continues to be an integral part of CARE III [10].

The second limitation was the assumption that fault-occurrence and fault-handling behavior are simultaneously accounted for by a single Markov model of system behavior. This implies a combinatorial explosion in the state space of the Markov chain, resulting in computation difficulties. It may be recognized, however, that the time constants of the fault-handling processes are several orders of magnitude smaller than those of the fault-occurrence events. It is therefore possible to analyze separately the fault-handling behavior of the system (the coverage model) and later incorporate the results of the coverage model, together with the fault-occurrence behavior, in an overall reliability model. This is the approach used in CARE III.

The third limitation was the assumption that all random variables of interest are exponentially distributed. In practice, this is seldom the case. One possible approach to the problem of non-exponential holding times is to use the method of stages [11]. Indeed, this approach has been used in other reliability models [12] and in queueing theoretic models for computer performance

evaluation [13]. However, the use of the method of stages increases the size of the state space. CARE III is a major departure from conventional approaches in that it purports to support non-exponential distributions, while avoiding the problem of large state spaces through the use of state aggregation. More specifically, CARE III uses a combination of semi-Markov techniques (while analyzing the coverage model) and time-dependent transition parameters resulting in a non-homogeneous Markov chain (at the aggregate model level).

In Section 2, we give some background regarding the ideas to be pursued in the remaining part of the paper. In Section 3 we present several simple examples illustrating important features of the CARE III model. In Section 4 we treat the CARE III model in a more general fashion with more detailed examples. In Section 5 several approximation techniques are discussed.

2. Background

A common approach to solving large problems is to partition the problem into smaller parts, and then combine the solutions of the parts into a solution for the entire problem. This approach to problem solving is known as divide-and-conquer and is considered to be very effective in designing alorithms [14]. The same approach is often found to be effective in solving large system analysis problems. In this connection we refer to the first step of dividing the original problem into smaller parts as decomposition and the step of combining solutions of parts into the solution for the whole as aggregation.

Aggregation and decomposition are simply the complementary activities of combining and separating parts of the system to facilitate analysis [15]. The decomposition/aggregation approach to system analysis will be effective if (i) interactions within a part can be studied as if interactions between parts did not exist and, (ii) interactions between parts can be analyzed without referring to the interactions within parts [16].

If we can assume that subsystem failure/recovery processes are independent of each other then a decomposition into subsystems, separate analysis of subsystems, and aggregation to obtain the final solution can be used. In CARE, for example, solution to subsystem reliability is obtained using the hybrid-NMR expression and the subsystem reliabilities are multiplied (aggregation step) to obtain system reliability.

Unfortunately the assumption of independent behavior of subsystems is often unrealistic. Nevertheless, if the coupling between subsystems is weak, we may consider the system nearly-decomposable [16] and the solution obtained by aggregation will then be an approximation to the desired solution. Indeed this approach is considered effective in queueing theoretic models of system performance analysis.

In the reliability context, however, there is an alternative approach to the above structural decomposition. This new approach may be called behavioral decomposition. We observe that the fault-occurrence behavior of a system is composed of relatively infrequent events while fault-handling behavior of a system is composed of

relatively frequent events. It may, therefore, be desirable to separately analyze the fault-handling behavior and reflect its effect in an aggregate model by one or more parameters. This is indeed the approach used in CARE II and CARE III. We must remember that the solution thus obtained will, in general, be an approximation to the desired solution. The behavioral approach to decomposition of complex reliability models will be explored further in the next two sections.

Next we should consider the problem of modeling non-exponential holding time distributions. By definition of a homogeneous Markov chain, the random variable denoting time spent in a state must have the memoryless property, that is, must be exponentially distributed. This implies a serious assumption about the behavior of various fault-occurrence and recovery processes, an assumption that is often violated.

In general, removing this restriction on holding times in the states of a Markov chain yields a semi-Markov process, with the corresponding difficulty in solving such models. At present, it appears that the use of general semi-Markov processes may have to be restricted to relatively small problems. Indeed, the coverage (fault-handling) model used in CARE II and CARE III uses the general semi-Markov approach.

The use of a general semi-Markov process implies that besides the state information, we must also have the time spent in the given state in order to predict the future behavior of the process. Thus, the effective state space is uncountably infinite. For most practical problems, however, a lot less information usually suffices. Besides

the state of the original stochastic process, a few bits of additional information regarding the time spent in the state is usually enough to predict the future. In other words, we still have a Markov chain with a finite (in general, countably infinite) state space, albeit a larger one than the original state space.

As a simple example of the problems involved in removing the exponential holding time assumption, consider a component with a constant failure rate λ (hence exponentially distributed time to failure). The Markov state diagram of the component is shown in Figure 1(a). This is a very simple model to solve for the state

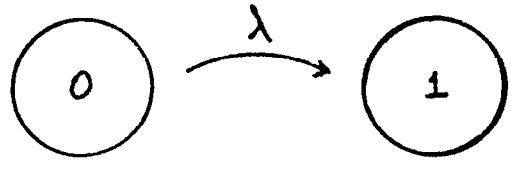

Figure 1(a) - Example Markov Chains.

probabilities and hence the component reliability. Now, suppose the assumption of exponentially distributed time to failure is unsatisfactory. Further suppose that the time to failure is a 2-stage Erlang random variable with parameter 2λ (hence the mean time to failure is the same as before, that is, $1/\lambda$). We can then model the behavior of the component using the three-state Markov chain as shown in Figure 1(b). In the state (0,A), the component is in failure free

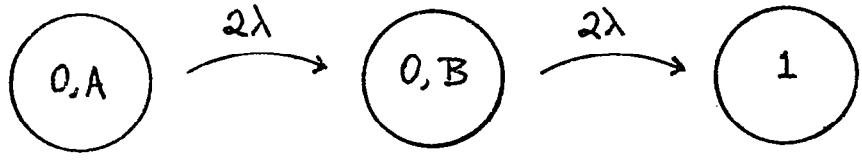

Figure 1(b)

state and in the first stage of its lifetime distribution. Since each stage of an Erlang random variable is exponentially distributed, each state of the resulting new state diagram possesses an exponentially distributed holding time. Furthermore, in general, given any holding time distribution, it is possible to derive an exponential stage type decomposition of that distribution to a specified degree of approximation [11]. The problem with this approach is that the more a given holding time differs from the exponential, the larger the number of stages needed to approximate it and the larger the state space of the resulting Markov chain.

Yet another approach to the problem of non-exponential holding times is to consider a Markov chain whose transition parameters are allowed to be time-dependent. The resulting Markov chain is said to be a non-homogeneous Markov chain. Thus, for example, the homogeneous Markov chain of Figure 1(a) is transformed into the non-homogeneous chain shown in Figure 1(c). It can be shown that the holding time distribution in state 0 is now given by

$$F_{X_0}(t) = 1 - e^{-\int_0^t \lambda(\tau)\, d\tau}$$

Note that if we let $\lambda(t) = at^b$, we have a Weibull holding time distribution.

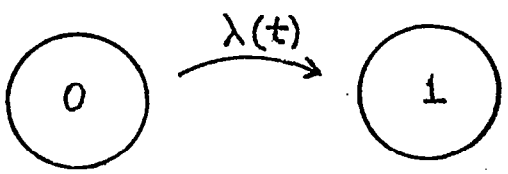

Figure 1(c)

Although solving for the state probabilities of a non-homogeneous Markov chain is somewhat more complex than solving for those of a homogeneous Markov chain, the advantage is that the state space is not expanded. Another disadvantage is that the transition rates are allowed to depend only on global time defined from the beginning of the process operation. In order to model an arbitrary holding time distribution in a given state i of the chain, we would like the transition parameter leading from state i to state j to be a function of local time, measured from the time of entry into state i. Since the (global) time of entry into state i is a random variable (unless state i is the start state), a simple shift of time origin is not adequate to transform local time based quantities into global time based quantities.

When we consider reliability models of systems without renewals (or repairs), the time to failure of a component can be measured in global time, and hence the failure rate leading out of state i can be labelled in terms of the global time. It is in this fashion that CARE III models non-exponential time-to-failure distributions at the aggregate model level.

Another apparent difficulty with this approach is met when we allow spare failure rates to be different from the failure rate of an active unit. Consider a 2-component standby redundant system with the active unit failure rate of $\lambda(t)$ and the passive unit failure rate $\alpha\lambda(t)$. The non-homogeneous Markov chain of Figure 1(d) is a model of this system assuming perfect coverage and further assuming that the failure rate of the spare unit once activated is only a function of its total age. This assumption is graphically depicted in Figure 1(e).

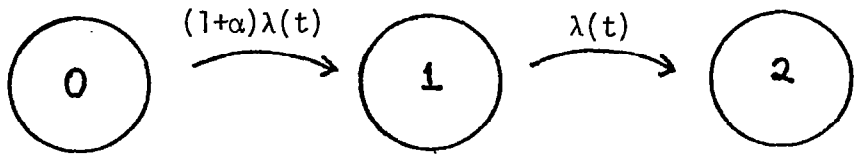

Figure 1(d)

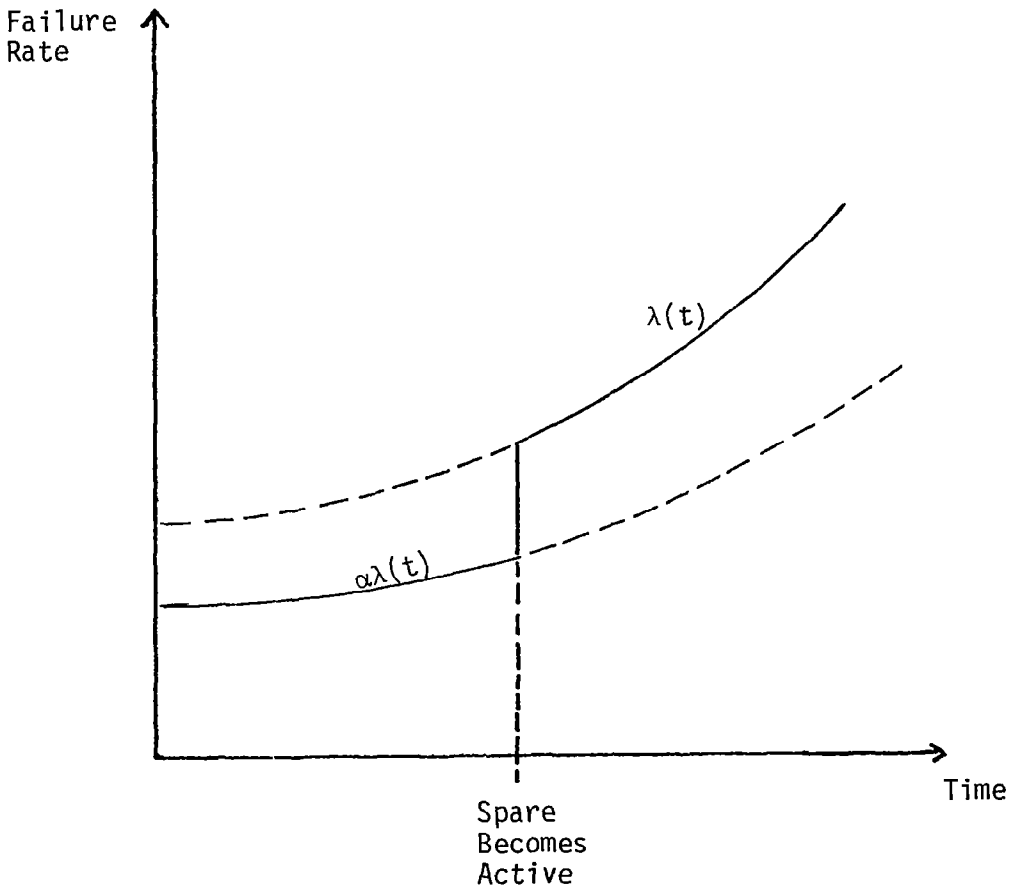

Figure 1(e)

Non-homogeneous Markov Chains

3. Motivating Examples

We shall now present the essential features of the CARE III model through a series of motivating examples.

Example 1: Consider a standby redundant system in which the failure rates of the spare and that of the active unit are both constant and equal to λ. Upon the occurrence of a failure, a recovery process takes control and with probability c succeeds in recovering from failure. The Markov state diagram of the system is shown in Figure 2.

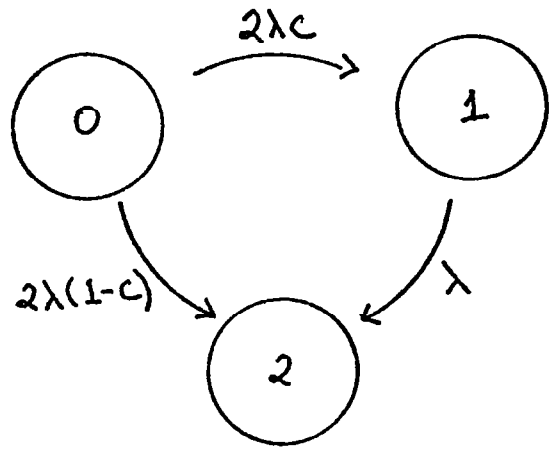

Figure 2. - Standby Redundant System Markov Chain

The standard approach to solve for the state probabilities of such a process is to set up Kolmogorov differential equations and (in the Markov case) use Laplace transforms to solve them. We will instead use convolution equations [17;pp.483-488] or the method of sample paths [18]. The reason for the use of this method is the easy generalization to non-Markovian (in particular, semi-Markov) processes which we will need shortly.

The integral equation for the transition probability $p_{ik}(t)$, the probability that the Markov chain is in state k at time t given that it started in state i at time 0, is given by

$$(1)\quad p_{ik}(t) = \delta_{ik}\, e^{-\lambda_i t} + \int_0^t \sum_j p_{ij}(x)\, \lambda_{jk}\, e^{-\lambda_k (t-x)}\, dx$$

where δ_{ik} is the Kronecker δ function (that is, $\delta_{ii} = 1$ and $\delta_{ik} = 0 \quad i \neq k$), λ_{ij} is the transition rate from state i to state j and $\lambda_i = \sum_j \lambda_{ij}$.

Applying Equation (1) to the current problem and remembering that the start state is 0 so that $P_0(0) = 1$, $P_i(0) = 0 \quad i \neq 1$, we have the equations for the state probabilities $P_k(t) = p_{0k}(t)$ as follows:

$$P_0(t) = e^{-2\lambda t},$$

$$P_1(t) = \int_0^t P_0(x)\, 2\lambda c\, e^{-\lambda(t-x)}\, dx$$

$$= 2\lambda\, c\, e^{-\lambda t} \int_0^t e^{-\lambda x}\, dx$$

$$= 2c\, [e^{-\lambda t} - e^{-2\lambda t}], \text{ and}$$

$$P_2(t) = \int_0^t P_0(x)\, 2\lambda(1-c)\, dx + \int_0^t P_1(x)\, \lambda\, dx$$

$$= \int_0^t e^{-2\lambda x}\, 2\lambda(1-c)\, dx + \int_0^t 2c\, [e^{-\lambda x} - e^{-2\lambda x}]\, \lambda\, dx$$

$$= (1-c)\, [1-e^{-2\lambda t}] + 2c\, [(1-e^{-\lambda t}) - \tfrac{1}{2}\, (1-e^{-2\lambda t})]$$

$$= 1 - 2c\, e^{-\lambda t} - (1-2c)\, e^{-2\lambda t}.$$

The system reliability

$$(2)\quad R(t) = \sum_{k \in L} P_k(t) = P_0(t) + P_1(t) = 2c\, e^{-\lambda t} + (1-2c)\, e^{-2\lambda t}$$

where $L = \{0,1\}$ is the set of system states where the system is functioning properly.

#

In Example 1, we note that the system reaches the failure state labelled 2 due to two distinct causes: exhaustion of spares, and coverage failure. For the subsequent discussion, we wish to separate the probabilities due to these two causes of failure.

Example 2: We reformulate the state diagram of Figure 2 so that the system has five states: in state 0 the system is functioning properly without any unit failing, in state 1G the system is functioning properly with a prior (covered) failure of one of the units, in state 1F the system has failed due to the occurrence of one uncovered failure, in state 2F the system has experienced two failures, in state 2G the system has experienced two failures (both covered) but the system has failed due to exhaustion of spares. The reformulated state diagram is shown in Figure 3.

The transition from state 1F to 2F may appear strange but it is very convenient. As we shall see in the next example, if we delete this transition, the state probabilities will change but the system reliability will be the same.

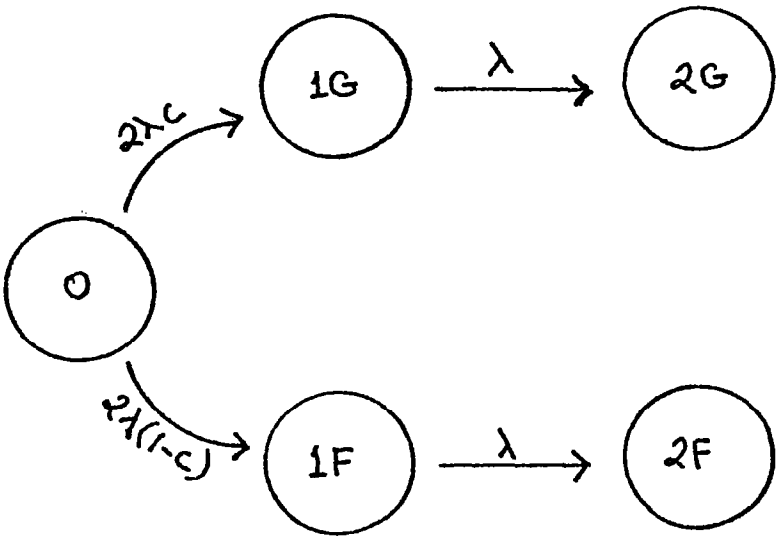

Figure 3. - Reformulated Figure 2 State Diagram

We will let

$$P_i(t) = P_{(iG)}(t) ,$$

$$Q_i(t) = P_{(iF)}(t), \text{ and}$$

$$P_i^*(t) = P_{(iG)}(t) + P_{(iF)}(t) .$$

Solving for the state probabilities, as in Example 1, we have

$$P_0(t) = e^{-2\lambda t} ,$$

$$P_1(t) = \int_0^t P_0(x)\ 2\lambda\ ce^{-\lambda(t-x)}\ dx$$

$$= 2c\ [e^{-\lambda t} - e^{-2\lambda t}] ,$$

$$Q_1(t) = \int_0^t P_0(x)\ 2\lambda(1-c)\ e^{-\lambda(t-x)}\ dx$$

$$= 2(1-c)\ [e^{-\lambda t} - e^{-2\lambda t}] ,$$

$$P_2(t) = \int_0^t P_1(x)\lambda\, dx$$

$$= c - 2c\, e^{-\lambda t} + c\, e^{-2\lambda t}, \text{ and}$$

$$Q_2(t) = \int_0^t Q_1(x)\, \lambda\, dx = (1-c) - 2(1-c)\, e^{-\lambda t} + (1-c)\, e^{-2\lambda t}$$

.

Note that the system reliability is given by

$$R(t) = \sum_{k \in L} P_k(t) = P_0(t) + P_1(t)$$

$$= 2c\, e^{-\lambda t} + (1-2c)\, e^{-2\lambda t},$$

as in Example 1 (Expression (2)).

Computing

$$P_0^*(t) = P_0(t) = e^{-2\lambda t}$$

$$P_1^*(t) = 2\, [e^{-\lambda t} - e^{-2\lambda t}], \text{ and}$$

$$P_2^*(t) = 1 - 2\, e^{-\lambda t} + e^{-2\lambda t},$$

we note that $P_i^*(t)$ is independent of the coverage factor c. But this should not be surprising if we redraw the state diagram of Figure 3 by aggregating states iG and iF into the state i^* to obtain the state diagram of Figure 4. Here all transition rates

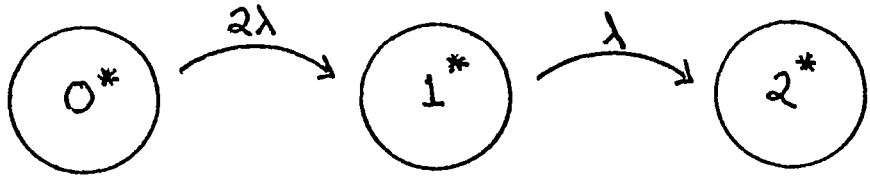

Figure 4. - Aggregated Figure 3 State Diagram.

are independent of c. Interpreting this diagram as the fictitious situation of perfect coverage, we conclude that $P_i^*(t)$ represents the probability that the system has sustained i faults by time t, assuming coverage to be perfect. This reinforces our earlier interpretation of $P_i(t)$ and $Q_i(t)$.

#

Example 3: Let us remove the assumption that a failure is allowed to occur in another module after an uncovered failure has occurred in some module. Therefore, we redraw the state

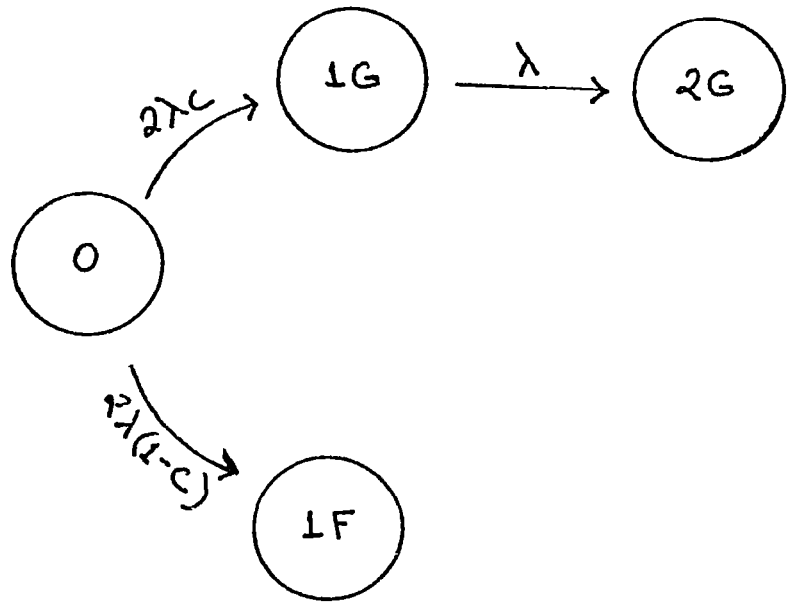

Figure 5. - Redrawn Figure 3 State Diagram.

diagram of Figure 3 as shown in Figure 5. Computing state probabilities, we get

$$P_0(t) = e^{-2\lambda t},$$

$$P_1(t) = P_{(1G)}(t) = 2c(e^{-\lambda t} - e^{-2\lambda t}),$$

$$Q_1(t) = P_{(1F)}(t) = \int_0^t P_0(x)\ 2\lambda(1-c)\ dx,$$

$$= (1-c)\ [1-e^{-2\lambda t}\ ],\ \text{and}$$

$$P_2(t) = P_{(2G)}(t) = c - 2ce^{-\lambda t} + c\ e^{-2\lambda t}\ .$$

Note that

$$R(t) = P_0(t)+P_1(t) = 2c\ e^{-\lambda t}+(1-2c)\ e^{-2\lambda t}$$

which is identical to the result obtained in Examples 1 and 2 (Expression (2)). However, we can no longer interpret $Q_j(t) + P_j(t) = P_j^*(t)$ as the probability of being in state j at time t were the coverage perfect.

#

One problem with models of Examples 1-3 is that the value of the coverage parameter c is assumed to be known (specified by the model user). In practice, however, such parameters are extremely difficult to estimate. The extreme sensitivity of the reliability to the coverage parameter [19] further compounds this problem. It is imperative, therefore, to provide a method of estimating coverage parameters based on more elementary, easier to specify, parameters.

Example 4: Consider the Markov model of the fault recovery process [20] shown in Figure 6. The model consists of five states. In the active state A, the fault is capable of producing errors at the rate ρ leading to the error state E. The fault is assumed to be an intermittent type so that occasionally it goes into the benign state B, where the affected circuitry temporarily functions correctly. In

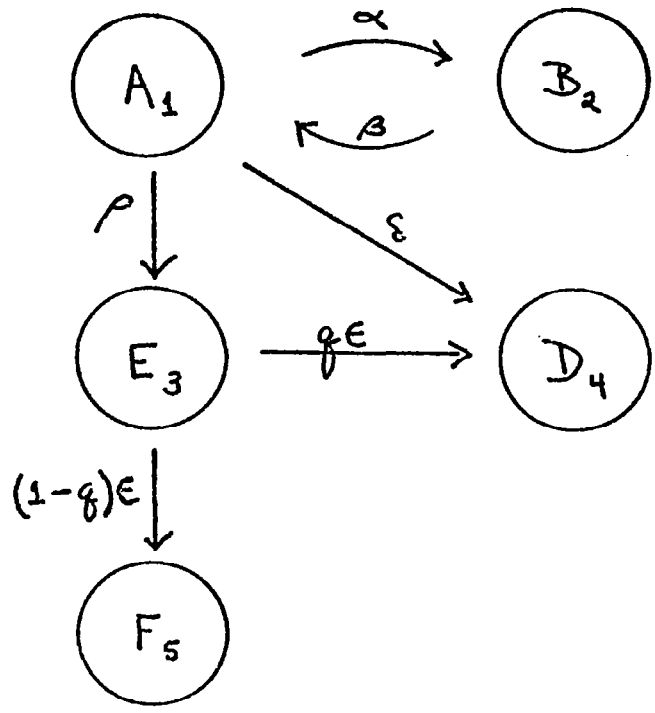

Figure 6. - Markov Model of Fault Recovery Process.

state D the fault has been detected while in state F, an undetected error has propagated so that we declare the system to have failed.

To illustrate the point of this example, it is more convenient to use the Laplace transform method to solve the differential equations for the Markov chain. First the differential equations are:

$$\frac{dP_1}{dt} = -(\alpha+\rho+\delta)\ P_1(t) + \beta\ P_2(t),$$

$$\frac{dP_2}{dt} = -\beta\ P_2(t) + \alpha\ P_1(t)\ ,$$

$$\frac{dP_3}{dt} = -\epsilon\ P_3(t) + \rho\ P_1(t)\ ,$$

$$\frac{dP_4}{dt} = \delta\ P_1(t) + q\ \epsilon\ P_3(t)\ ,\ \text{and}$$

$$\frac{dP_5}{dt} = (1-q)\ \epsilon\ P_3(t)\ .$$

Applying Laplace transforms and recalling that state 1 is the initial state, we get ($\bar{P}_i(s)$ denotes the Laplace transform of $P_i(t)$):

$$(s\,\bar{P}_1(s)-1) = -(\alpha+\rho+\delta)\,\bar{P}_1(s) + \beta\,\bar{P}_2(s)$$

or

$$\bar{P}_1(s) = \frac{\beta\,\bar{P}_2(s)+1}{s+\alpha+\rho+\delta},$$

$$\bar{P}_2(s) = \frac{\alpha\bar{P}_1(s)}{s+\beta},$$

$$\bar{P}_3(s) = \frac{\rho\,\bar{P}_1(s)}{s+\epsilon},$$

$$\bar{P}_4(s) = \frac{\delta\,\bar{P}_1(s)+q\,\epsilon\,\bar{P}_3(s)}{s}, \text{ and}$$

$$\bar{P}_5(s) = (1-q)\,\epsilon\,\frac{\bar{P}_3(s)}{s}.$$

Hence,

$$\bar{P}_1(s) = \frac{1}{s+(\alpha+\rho+\delta) - \frac{\alpha\beta}{s+\beta}}$$

and $$\bar{P}_4(s) = \frac{1}{s}\left(\delta+\frac{q\,\epsilon\rho}{s+\epsilon}\right)\left(\frac{1}{(s+\alpha+\rho+\delta) - \frac{\alpha\beta}{s+\beta}}\right).$$

Although it is possible to invert this transform to obtain the probability of detection by time t, $P_4(t)$, we will be content here with finding the limiting probability by using the Final Value Theorem of Laplace Transform:

$$\lim_{t\to\infty} P_4(t) = \lim_{s\to 0} s\,\bar{P}_4(s) = \left(\delta+\frac{q\epsilon\,\rho}{\epsilon}\right)\frac{1}{(\alpha+\rho+\delta)-\alpha}$$

$$= \frac{\delta+\rho\,q}{\delta+\rho}$$

This represents the probability that the fault (which occurred at time t=0) eventually is detected. It is for this reason that we conclude that the coverage factor for this fault model is given by

$$(3)\quad c = \frac{\delta+\rho\,q}{\delta+\rho}.$$

Similarly, $(1-c) = \lim_{t\to\infty} P_5(t) = \frac{\rho(1-q)}{\delta+\rho}$.

#

Example 5: The results of Example 4 can be used to calculate the coverage factor c, and subsequently this value of c can be used in the computations of Example 1 (or 2 or 3) in order to evaluate the system reliability. Now the user can specify elemental quantities δ ,ρ ,q, α ,β as needed in the coverage model calculations. Thus, for instance, the reliability model of Example 2 in conjunction with the coverage model of Example 4 gives the following state probabilities:

$$P_0(t) = e^{-2\lambda t}\ ,$$

$$(4)\quad P_1(t) = 2\,\frac{\delta+\rho\,q}{\delta+\rho}\,[e^{-\lambda t} - e^{-2\lambda t}]\ ,$$

$$(5)\quad Q_1(t) = 2\,\frac{\rho(1-q)}{\delta+\rho}\,[e^{-\lambda t} - e^{-2\lambda t}]\ ,$$

$$(6)\quad P_2(t) = \frac{\delta+\rho\,q}{\delta+\rho}\,[1 - 2e^{-\lambda t} + e^{-2\lambda t}]\ ,$$

(7) $Q_2(t) = \frac{\rho(1-q)}{\delta+\rho}\left[1 - 2e^{-\lambda t} + e^{-2\lambda t}\right]$, and system reliability,

(8) $R(t) = e^{-2\lambda t} + 2\frac{\delta+\rho\, q}{\delta+\rho}\left(e^{-\lambda t} - e^{-2\lambda t}\right)$.

#

Use of the hierarchical approach to reliability evaluation described so far is supported by a realization that holding times in various states of the coverage model (of Example 4) will be several orders of magnitude smaller than those in the fault-occurrence models (Examples 1-3). Nevertheless, this approach yields only a first-order approximation to the more accurate model that we wish to study.

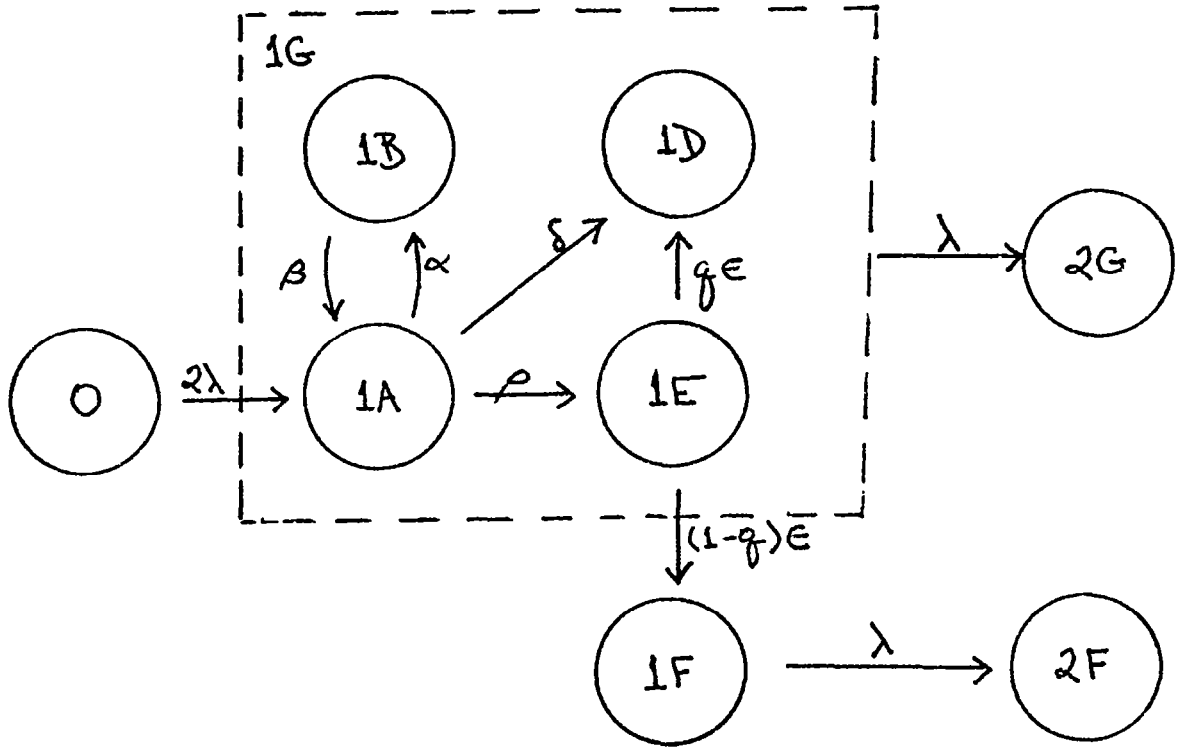

Figure 7. - Markov Model of a Two-Unit System.

Example 6: Consider the Markov reliability model of a 2-unit system as shown in Figure 7. Solving for the state probabilities of

this Markov chain using the convolution integration approach we get (for the sake of simplicity we assume that $\alpha = \beta = 0$):

$$P_0(t) = e^{-2\lambda t} ,$$

$$P_{(1A)}(t) = \int_0^t P_0(x)\, 2\lambda e^{-(\delta+\rho+\lambda)(t-x)}\, dx$$

$$= \frac{2\lambda}{\lambda-(\delta+\rho)} e^{-(\delta+\rho+\lambda)t} - \frac{2\lambda}{\lambda-(\delta+\rho)} e^{-2\lambda t} ,$$

$$P_{(1E)}(t) = \int_0^t P_{(1A)}(x)\, \rho e^{-(\epsilon+\lambda)(t-x)}\, dx$$

$$= \frac{2\lambda\rho\, e^{-(\epsilon+\lambda)t}}{(\delta+\rho-\epsilon)(\lambda-\epsilon)} - \frac{2\lambda\rho e^{-(\delta+\rho+\lambda)t}}{(\lambda-(\delta+\rho))(\delta+\rho-\epsilon)} + \frac{2\lambda\rho\, e^{-2\lambda t}}{(\lambda-(\delta+\rho))(\lambda-\epsilon)} ,$$

$$P_{(1D)}(t) = \int_0^t P_{(1A)}(x)\delta e^{-\lambda(t-x)}dx + \int_0^t P_{(1E)}(x) q\, \epsilon e^{-\lambda(t-x)}dx$$

$$= \frac{2(\delta+\rho q)}{(\delta+\rho)} e^{-\lambda t}$$

$$+ \left[\frac{2\lambda(\rho\, q)\epsilon}{(\delta+\rho)(\delta+\rho-\epsilon)(\lambda-(\delta+\rho))} - \frac{2\lambda\delta}{(\lambda-(\delta+\rho))(\delta+\rho)}\right] e^{-(\lambda+\delta+\rho)t}$$

$$- \frac{2\lambda\rho\, q e^{-(\lambda+\epsilon)t}}{(\delta+\rho-\epsilon)(\lambda-\epsilon)}$$

$$- \left[\frac{2(\delta+\rho q)\,\epsilon}{(\lambda-\epsilon)(\lambda-(\delta+\rho))} - \frac{2\delta\lambda}{(\lambda-(\delta+\rho))(\lambda-\epsilon)}\right] e^{-2\lambda t} ,$$

$$P_{(1F)}(t) = \int_0^t P_{(1E)}(x)\, (1-q)\, \epsilon\, e^{-\lambda(t-x)}\, dx$$

$$= \frac{2\rho(1-q)\, e^{-\lambda t}}{\delta+\rho} - \frac{2\lambda(1-q)\,\rho}{(\delta+\rho-\epsilon)(\lambda-\epsilon)} e^{-(\lambda+\epsilon)t} + \frac{2\lambda\rho(1-q)\,\epsilon e^{-(\lambda+\delta+\rho)t}}{(\lambda-(\delta+\rho))(\delta+\rho-\epsilon)(\delta+\rho)}$$

$$- \frac{2\,\rho(1-q)\,\epsilon\, e^{-2\lambda t}}{(\lambda-\epsilon)(\lambda-(\delta+\rho))} ,$$

$$P_{(2F)}(t) = \int_0^t P_{(1F)}(x)\lambda\, dx$$

$$= \frac{\rho\epsilon(1-q)\left[(\rho+\delta)^2+(\rho+\delta)(\lambda+\epsilon)+\lambda\epsilon\right]}{(\rho+\delta-\lambda)(\rho+\delta-\epsilon)(\rho+\delta+\lambda)(\lambda+\epsilon)} - \frac{2\rho(1-q)}{(\rho+\delta)}e^{-\lambda t}$$

$$+ \frac{2\rho\lambda^2(1-q)}{(\lambda^2-\epsilon^2)(\rho+\delta-\epsilon)} - \frac{2\rho\lambda^2\epsilon(1-q)}{(\lambda+\rho+\delta)(\lambda-(\rho+\delta))(\rho+\delta-\epsilon)(\rho+\delta)}e^{-(\lambda+\rho+\delta)t}$$

$$+ \frac{\rho(1-q)\epsilon}{(\lambda-\epsilon)(\lambda-(\rho+\delta))}e^{-2\lambda t},$$

and

$$P_{(2G)}(t) = \int_0^t \left[P_{(1A)}(x)+P_{(1D)}(x)+P_{(1E)}(x)\right]\lambda\, dx\ .$$

$$= 1-(P_0+P_{1A}+P_{1E}+P_{1D}+P_{1F}+P_{2F})\ .$$

In our earlier terminology, we are now in a position to compute $Q_1(t) = P_{(1F)}(t)$:

$$(9)\quad Q_1(t) = \frac{2\rho(1-q)}{\delta+\rho}\left[e^{-\lambda t} - \frac{\epsilon(\delta+\rho)}{(\lambda-\epsilon)(\lambda-(\delta+\rho))}e^{-2\lambda t}\right]$$

$$- \frac{2\lambda\rho(1-q)}{(\delta+\rho-\epsilon)}\left[\frac{e^{-(\lambda+\epsilon)t}}{\lambda-\epsilon} - \frac{\epsilon\, e^{-(\lambda+\delta+\rho)t}}{[\lambda-(\delta+\rho)](\delta+\rho)}\right].$$

Comparing Expression (9) with the earlier Expression (5) derived in Example 5, we note that if we let λ/ϵ and $\lambda/(\delta+\rho)$ approach zero while keeping the individual terms non-zero, the two expressions become identical in the limit. A similar argument will show that in the limit all state probabilities derived in the present example reduce to those derived in Example 5. Thus indeed, the approach in Example 5

is a first-order approximation to the exact solution derived above. For instance let us compute

$$(10)\quad P_1(t) = P_{(1A)}(t)+P_{(1B)}(t)+P_{(1D)}(t)+P_{(1E)}(t)$$

$$= \frac{2(\delta+\rho q)}{\delta+\rho} e^{-\lambda t}$$

$$- \left[\frac{2[(\lambda-\epsilon)(\lambda-\delta)-\rho(\lambda-q\epsilon)]}{(\lambda-\epsilon)(\lambda-(\rho+\delta))}\right] e^{-2\lambda t} + \frac{2\lambda\rho(1-q)e^{-(\lambda+\epsilon)t}}{(\delta+\rho-\epsilon)(\lambda-\epsilon)}$$

$$+ \frac{2\lambda[\epsilon\rho(q-1)]}{(\delta+\rho)(\delta+\rho-\epsilon)(\lambda-(\delta+\rho))} e^{-(\lambda+\delta+\rho)t} .$$

In modeling ultra-high reliability systems the approximate approach of Example 5 may not be adequate but, at the same time, the exact approach of Example 6 can become unmanageable when we consider systems with hundreds or thousands of modules. We therefore need to pursue decomposition approaches which are more accurate than the first-order approach of Example 5, yet more manageable than the exact solution of Example 6. CARE III provides one such approach to handling reliability models with an extremely large number of states.

#

Example 7: Continuing with the Markov chain of Example 6, suppose we wish to suppress all the details of various states of the coverage model, and, with a given number of faults join the system, we consider only 2 states: the system has experienced a coverage failure or it has not. In the

specific case at hand, we aggregate the states 1A, 1B, 1D, and 1E into a single state 1G as shown in Figure 8.

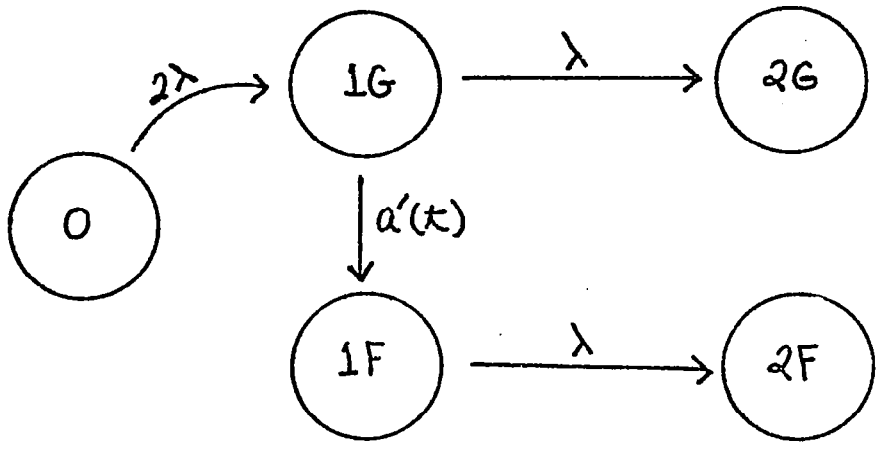

Figure 8. - State Aggregation for Example 6.

In order to complete the specification of this reduced Markov chain, we need to specify the transition parameter a'(t). We shall see shortly that this parameter is time dependent (as indicated by the notation) and hence the Markov chain of Figure 8 is non-homogeneous.

The easiest way to compute a'(t) is to refer back to the solution of the Markov chain of Figure 6:

$$a'(t) = \frac{(1-q)\,\epsilon P_{(1E)}(t)}{P_{(1A)}(t)+P_{(1B)}(t)+P_{(1D)}(t)+P_{(1E)}(t)} \quad .$$

In other words, to compute the effective transition rate from an aggregate state, we sum the transition rate times the state probability of each state contributing to the outward flow in the non-reduced model and divide the sum by

the total probability of being in any one of the aggregated states. In the present case, we get

$$a'(t) = \frac{(1-q)\epsilon\left[\frac{2\lambda\rho e^{-(\epsilon+\lambda)t}}{(\delta+\rho-\epsilon)(\lambda-\epsilon)} - \frac{2\lambda\rho\, e^{-(\delta+\rho+\lambda)t}}{(\lambda-(\delta+\rho))(\delta+\rho-\epsilon)} + \frac{2\lambda\rho e^{-2\lambda t}}{(\lambda-(\delta+\rho))(\lambda-\epsilon)}\right]}{P_1(t)}$$

where $P_1(t)$ is given by (10).

Dividing the numerator and denominator by $2\, e^{-\lambda t}$, we obtain

(11)

$$a'(t) = \frac{(1-q)\epsilon\left[\frac{\lambda\rho e^{-\epsilon t}}{(\delta+\rho-\epsilon)(\lambda-\epsilon)} - \frac{\lambda\rho\, e^{-(\delta+\rho)t}}{(\lambda-(\delta+\rho))(\delta+\rho-\epsilon)} + \frac{\lambda\rho e^{-\lambda t}}{(\lambda-(\delta+\rho))(\lambda-\epsilon)}\right]}{c - \left[\frac{(\lambda-\epsilon)(\lambda-\delta)-\rho(\lambda-q\epsilon)}{(\lambda-\epsilon)(\lambda-(\rho+\delta))}\right] e^{-\lambda t} + \left[\frac{\lambda\rho(1-q)}{(\rho+\delta-\epsilon)(\lambda-\epsilon)}\right] e^{-\epsilon t} + \left[\frac{\lambda(\epsilon\rho(q-1))}{(\delta+\rho)(\delta+\rho-\epsilon)(\lambda-(\delta+\rho))}\right] e^{-(\rho+\delta)t}}$$

where, again, $c = \frac{\delta+\rho\, q}{\delta+\rho}$.

#

Now all the transition parameters of the non-homogeneous Markov chain of Figure 8 have been obtained and hence the state probabilities can easily be found using standard methods (to be described in the next section). However, there is a catch in this procedure! Before we solve the reduced model of Figure 8, we must first solve the full model of Example 6 in order to obtain the transition parameter a'(t)! Nothing seems to be gained by the process

of reduction. The answer to this objection is that the computation of a'(t) can be carried out without solving the full reliability model. In fact, in computing a'(t) we need only to look at a very simple coverage model (with 5 states in the present case) and then solve the fault model of Figure 8 (also with 5 states in the present case). This computation replaces the earlier computation based on the model of Figure 6 (with 8 states).

Example 8: We now proceed to illustrate the computation of a'(t) using the coverage model of Figure 9. We note that the coverage

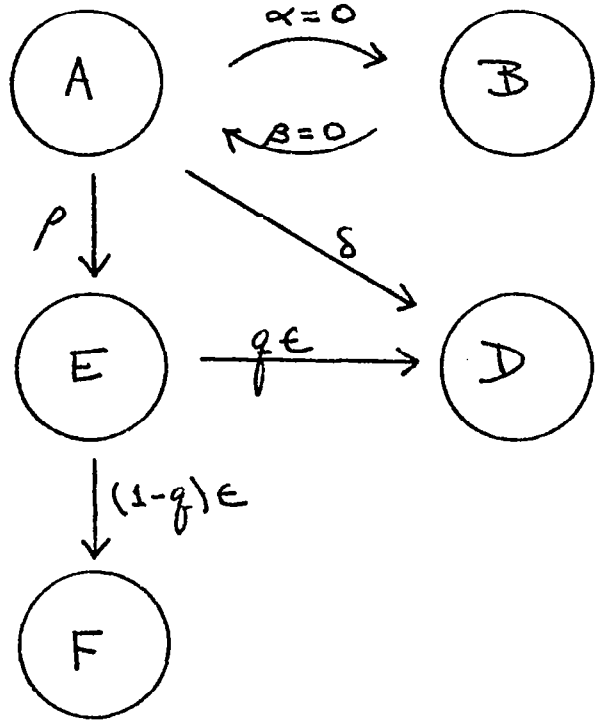

Figure 9. - Coverage Model for a'(t) Computation.

model will be entered subsequent to a failure in one of the two modules at some time τ. Let $p_j(t-\tau)$ denote the probability of being in state $j \in \{A,B,D,E,F\}$ at time t given that the coverage model was entered at time τ. We

compute these probabilities using the convolution integration approach:

$$p_A(t-\tau) = e^{-(\delta+\rho)(t-\tau)}$$

$$p_E(t-\tau) = \int_0^{t-\tau} p_A(x)\rho\, e^{-\epsilon(t-\tau-x)}\, dx$$

$$= \frac{\rho}{\delta+\rho-\epsilon}\left(e^{-\epsilon(t-\tau)} - e^{-(\delta+\rho)(t-\tau)}\right),$$

$$p_D(t-\tau) = \int_0^{t-\tau} (p_A(x)\delta + p_E(x)\, q\, \epsilon)\, dx$$

$$= \frac{\delta+\rho q}{\delta+\rho} - \frac{\rho q}{(\delta+\rho-\epsilon)} e^{-\epsilon(t-\tau)} + \frac{\epsilon(\delta+\rho q)-\delta(\delta+\rho)}{(\delta+\rho)(\delta+\rho-\epsilon)} e^{-(\delta+\rho)(t-\tau)}$$

and

$$p_F(t-\tau) = \int_0^{t-\tau} p_E(x)(1-q)\,\epsilon\, dx$$

$$= \frac{(1-q)\rho}{\rho+\delta} - \frac{(1-q)\rho}{\rho+\delta-\epsilon} e^{-\epsilon(t-\tau)} + \frac{(1-q)\epsilon\rho}{(\rho+\delta-\epsilon)(\rho+\delta)} e^{-(\rho+\delta)(t-\tau)}$$

In order to compute a'(t), we note that

#

$$a'(t) = \frac{(1-q)\epsilon^* \text{ Prob. of being in state E at time t}}{\text{Prob. of being in one of the states } \{A,B,D,E\} \text{ at time t}}$$

$$= \frac{(1-q)\epsilon \int_0^t p_E(t-\tau)^* \text{ P(cov. model entered in the interval } (\tau,\tau+d\tau))}{\int_0^t [p_A(t-\tau)+p_B(t-\tau)+p_D(t-\tau)+p_E(t-\tau)]^* \text{P(cov. model entered in the interval } (\tau,\tau+d\tau))}$$

$$= (1-q)\epsilon \frac{\int_0^t p_E(t-\tau)\lambda e^{-\lambda\tau} d\tau}{\int_0^t (1-p_F(t-\tau))\,\lambda e^{-\lambda\tau} d\tau} = \frac{(1-q)\epsilon N}{D}$$

First evaluate the numerator N,

$$N = \int_0^t \frac{\rho}{\delta+\rho-\epsilon}\left[e^{-\epsilon(t-\tau)} - e^{-(\delta+\rho)(t-\tau)}\right]\lambda\, e^{-\lambda\tau} d\tau$$

$$= \frac{\lambda\rho e^{-\epsilon t}}{(\delta+\rho-\epsilon)(\lambda-\epsilon)} + \frac{\lambda\rho e^{-\lambda t}}{(\lambda-\epsilon)(\lambda-(\delta+\rho))} - \frac{\lambda\rho e^{-(\delta+\rho)t}}{(\delta+\rho-\epsilon)(\lambda-(\delta+\rho))}$$

In a similar fashion, D is computed and to our pleasant surprise, we find that the ratio $\frac{(1-q)\epsilon N}{D}$ exactly matches with our earlier expression for a'(t) given by (11).

#

The method described in the last example can be extended to more complex coverage models, and the results of the coverage model calculations can then be plugged into the overall reliability model which will necessarily be a non-homogeneous Markov chain. These extensions are developed in the next section.

4. CARE III Model Development

As pointed out in the last section, two major concerns with any advanced reliability prediction model are:

1) the problem of very large state spaces, and
2) the desire to include non-exponential holding times.

The CARE III approach to the first problem is the state aggregation (or decomposition) method, and the approach to the second uses a combination of semi-Markov techniques (at the coverage model level) and time-dependent transition parameters resulting in a non-homogeneous Markov chain (at the aggregate model level).

As noted earlier, non-exponential holding times within the coverage model are handled using the sample path enumeration method. Let us examine the approach of non-homogeneous Markov chains used in CARE III to deal with non-exponential holding times in states outside the coverage model. As seen in Example 7, even if all holding times are assumed to be exponentially distributed in the original model, derived transition parameters of the aggregate model are time dependent, hence the temptation occurs to use time-dependent transition parameters to model non-exponential holding times in the fault-occurrence model.

One problem occurs in using this approach. The time dependency of transition parameters can be easily handled, provided the time is measured from the beginning of system operation (global time). However, non-exponential holding times in a state naturally give rise to time-dependent transition parameters associated with all arcs emanating from the state, with time measured from the point of entry into that state (local time). Suppose, for example, we wish to model the holding time in state i to be Weibull distributed with the hazard rate $\lambda(\tau) = a\,\tau^b$, and suppose there is only one transition out of state i to state j; then we must label the (i,j) transition with parameter $\lambda_{ij}(\tau) = a\,\tau^b$ where time τ is measured from the time of the last entry into state i. Now the global t is related to τ by $t = T_i + \tau$ where T_i is the global time to the last entry into state i. Note that T_i is a random variable and hence a fixed time translation will not suffice, in general.

The argument to be used here in favor of CARE III is that all failure processes can be assumed to start at the beginning of system operation; hence, the global time can be used to assign time-dependent transition rates to all arcs due to failure events. Of course, this argument breaks down if renewals (repairs) take place. However, as per the interpretation in Section 2 (Figures 1(d) and 1(e)) non-unity dormancy factor (that is, spare failure rate being different from active failure rate) can be handled.

We will develop the general approach to non-homogeneous Markov chains and its use in the CARE III model in the next three subsections.

4.1 Non-Homogeneous Markov Chains

Consider a discrete-state continuous parameter Markov chain $\{X(t),\ t \geq 0\}$. Let the transition probabilities

$$p_{ij}(v,t) = P(X(t)=j \mid X(v) = i)$$

for $0 \leq v \leq t$ and $i,j = 0,1,2,\ldots$

where we define

$$p_{ij}(t,t) = \begin{cases} 1 & , \text{ if } i=j \\ 0 & , \text{ otherwise} \end{cases} .$$

The Markov chain $\{X(t),\ t \geq 0\}$ is said to be (time)-homogeneous (or is said to have stationary transition probabilities) if $p_{ij}(v,t)$ depends only on the time difference $(t-v)$. Let us denote the state probabilities at time t by

$$P_k(t) = P(X(t)=k) \quad , k=0,1,2,\ldots \text{ and } t \geq 0 .$$

We assume that state 0 is the initial state and hence,

$$P_k(t) = p_{0k}(0,t) \ .$$

The transition probabilities of a Markov chain $\{X(t), t \geq 0\}$ satisfy the Chapman-Kolmogorov Equation [21]: for all i, j in the state space,

$$(12) \quad p_{ij}(v,t) = \sum_{k \in I} p_{ik}(v,u)\, p_{kj}(u,t) \quad 0 \leq v < u < t.$$

The direct use of (12) is difficult. The state probabilities are usually obtained by solving a system of differential equations that we derive next. Under certain regularity conditions, we can show that for each j there is a non-negative continuous function $q_j(t)$ defined by

$$q_j(t) = \frac{\partial}{\partial t} p_{jj}(v,t) \Big|_{v=t}$$
$$= \lim_{h \to 0} \frac{p_{jj}(t,t) - p_{jj}(t,t+h)}{h} = \lim_{h \to 0} \frac{1 - p_{jj}(t,t+h)}{h} \ .$$

Similarly for each i and j ($\neq$i) there is a non-negative continuous function $q_{ij}(t)$ defined by

$$q_{ij}(t) = \frac{\partial}{\partial t} p_{ij}(v,t) \Big|_{v=t}$$
$$= \lim_{h \to 0} \frac{p_{ij}(t,t+h) - p_{ij}(t,t)}{h} = \lim_{h \to 0} \frac{p_{ij}(t,t+h)}{h} \ .$$

Then the transition probabilities and the transition rates are related by[1]:

$$p_{ij}(t,t+h) = q_{ij}(t) * h+o(h) , \quad i \neq j$$

and

$$p_{jj}(t,t+h) = 1 - q_j(t) * h+o(h) , \quad i=j .$$

Using (12), it is possible to obtain a differential equation for the state probability $P_j(t)$:

$$(13) \quad \frac{d P_j}{dt} = [\sum_{i \neq j} P_i(t) \, q_{ij}(t)] - P_j(t) \, q_j(t) .$$

The linear first-order differential equation is easily solved using standard calculus techniques [22, pp. 53-57] to obtain the convolution integral form of $P_j(t)$ (analogous to Equation (1) for the homogeneous case):

$$(14) \quad P_j(t) = P_j(0) e^{-\int_0^t q_j(\tau) d\tau} + \sum_{i \neq j} \int_0^t P_i(x) q_{ij}(x) e^{-\int_x^t q_j(\tau) d\tau} dx .$$

The first term on the right-hand side will be zero for all but the initial state.

---

[1] $o(h)$ is any function of h that approaches zero faster than h:

$$\lim_{h \to 0} \frac{o(h)}{h} = 0 .$$

Example 9: Consider the slightly general version of the Markov chain in Figure 4, shown in Figure 10. Applying Equation (14), we get various state probabilities:

$$P_0^*(t) = e^{-2\int_0^t \lambda(\tau)\,d\tau},$$

$$P_1^* = \int_0^t P_0^*(x)\ 2\lambda(x)\ e^{-\int_x^t \lambda(\tau)\,d\tau}\,dx\ , \text{ and}$$

$$P_2^* = \int_0^t P_1^*(x)\ \lambda(x)\ dx\ .$$

Given the function $\lambda(t)$, it is possible to numerically evaluate the state probabilities in order $P_0^*(t)$, $P_1^*(t)$, $P_2^*(t)$. We will assume that our aggregate reliability models will not have any renewals or repair type transitions; it will always be possible to order the states in this fashion. It should be noted that the Markov chain of Figure 10 represents the twice collapsed version of the Markov chain of Figure 7. The first level of collapsing was done to Figure 8; now if we further collapse states 1G and 1F into state 1^*, states 2G and 2F into state 2^*, and relabel state 0 as 0^*, we obtain the diagram of Figure 10 (albeit, with the addition of time-dependent transition rates).

#

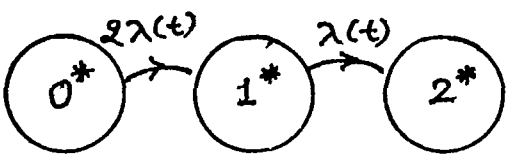

Figure 10. - Generalized Figure 4 Markov Chain.

With CARE III models, it is always the case that the reliability model under the assumption of perfect coverage will be a generalized version of the model in Example 9. Furthermore, we will need the state probabilities for the perfect coverage case in order to evaluate the state probabilities of the model with imperfect coverage.

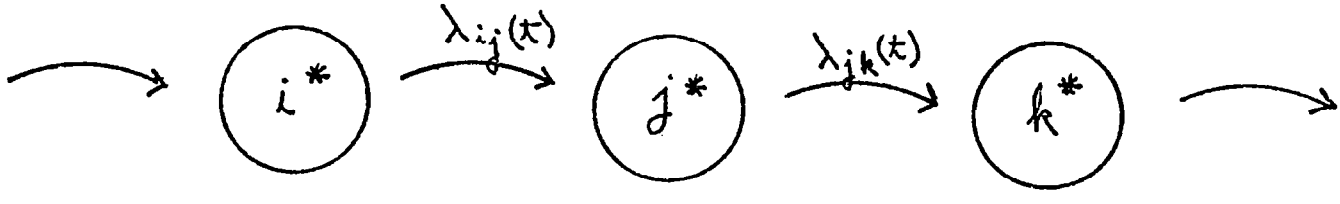

Figure 11. - Perfect Coverage Case.

In the perfect coverage case, we let $\lambda_{ij}(t)$ denote the transition rate from state i to state j (due to a failure event) and let $\lambda_i(t) = \sum_j \lambda_{ij}(t)$ (see Figure 11). Then the state probabilities are written as:

$$(14a)\quad P_j^*(t) = P_j^*(0)\, e^{-\int_0^t \lambda_j(\tau)d\tau} + \sum_{i\neq j} \int_0^t P_i^*(x)\lambda_{ij}(x)\, e^{-\int_x^t \lambda_j(\tau)d\tau}\, dx\ .$$

4.2 Reliability Models with Imperfect Coverage

The general structure of an aggregate CARE III model is shown in Figure 12. The perfect-coverage version of this chain, with states jG and jF collapsed into state j^*, is shown in Figure 11, where we necessarily have

$$(15)\quad \lambda_j(t) = \sum_k \lambda_{jk}(t) = \eta_j(t) + \sum_k \gamma_{jk}(t) + \sum_k \theta_{jk}(t)\ .$$

The $\eta_j(t)$ transitions are due to preexisting latent faults that cause a coverage failure without additional faults occurring. The $\Theta_{ij}(t)$ transitions are due to the occurrence of a fault that either by itself or in conjunction with preexisting latent faults, causes an immediate coverage failure.

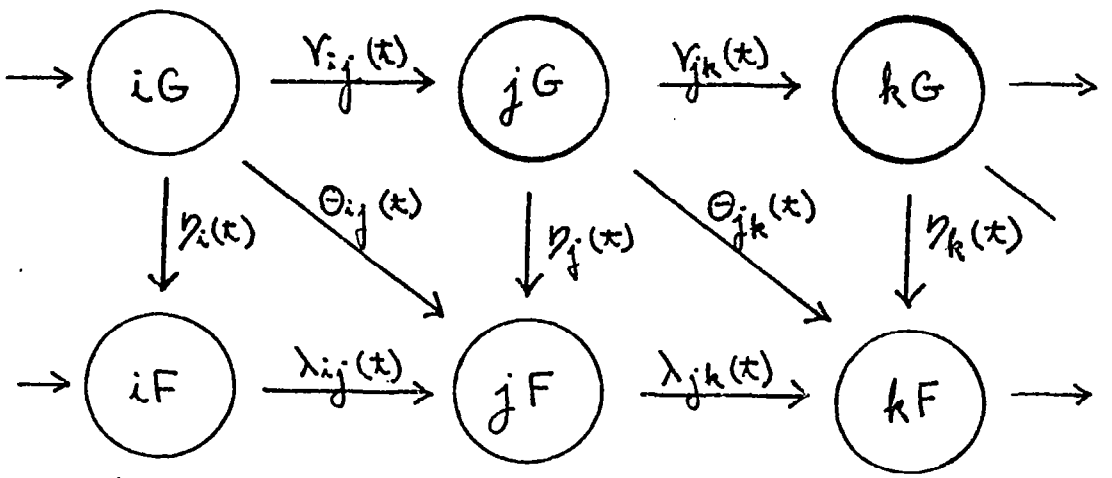

Figure 12. - General Structure of CARE III Aggregate Model.

Using the convolution integration approach (14), we can write the state probabilities:

(16a)

$$P_j(t)=P_{(jG)}(t)=P_j(0)\ e^{-\int_0^t \lambda_j(\tau)d\tau} + \sum_{i\neq j} \int_0^t P_i(x)\ \gamma_{ij}(x)\ e^{-\int_x^t \lambda_j(\tau)d\tau}\ dx$$

and

(16b)

$$Q_j(t)=P_{(jF)}(t) = \sum_{i\neq j} \int_0^t Q_i(x)\lambda_{ij}(x)\ e^{-\int_x^t \lambda_j(\tau)d\tau}\ dx + \sum_{i\neq j} \int_0^t P_i(x)\ \Theta_{ij}(x)\ e^{-\int_x^t \lambda_j(\tau)d\tau}\ dx + \int_0^t P_j(x)\eta_j(x)\ e^{-\int_x^t \lambda_j(\tau)d\tau}\ dx .$$

For numerical reasons, ($Q_j(t)$ is typically close to 0, while $P_j(t)$ is close to 1) the computations of $Q_j(t)$ (using (16b)) were found to be less prone to round-off error accumulation than those of $P_j(t)$ (using (16a)). Further, although the $Q_j(t)$ depends directly upon $P_j(t)$, it has been the experience of the implementors of CARE III that replacing $P_j(t)$ by $P_j^*(t)$ in the Equation (16b) for $Q_j(t)$ does not cause excessive errors, and those introduced are on the conservative side of <u>under</u>- estimating system reliability. Therefore, we can write

$$(17)\quad Q_j(t) \cong \sum_{i\neq j} \int_0^t Q_i(x)\lambda_{ij}(x)\, e^{-\int_x^t \lambda_j(\tau)d\tau}\, dx + \sum_{i\neq j} \int_0^t P_i^*(x)\,\theta_{ij}(x)\, e^{-\int_x^t \lambda_j(\tau)d\tau}\, dx + \int_0^t P_j^*(x)\eta_j(x)\, e^{-\int_x^t \lambda_j(\tau)d\tau}\, dx\ .$$

Thus, we first compute $P_j^*(t)$ (perfect-coverage case; using Equation (14a)) and then compute $Q_j(t)$ using the above approximation (17). The system reliability is given by

$$R(t) = 1-\Big(\sum_{j\in L} Q_j(t) + \sum_{j\in \bar{L}} P_j(t)\Big)$$

$$= 1-\Big(\sum_{j\in L} Q_j(t) + \sum_{j\in \bar{L}} P_j^*(t) - \sum_{j\in \bar{L}} Q_j(t)\Big)$$

where L is the set of good (system operational, given perfect coverage) states and $\bar{L}$ is the set of bad states.

Before calculation of $Q_j(t)$ can be carried out, the transition parameters $\lambda_{ij}(t)$, $\Theta_{ij}(t)$, $\gamma_{ij}(t)$, and $\eta_j(t)$ have to be specified. Of these, $\lambda_{ij}(t)$ will be user specified, and the remaining parameters will be computed based upon the user specified coverage and failure rate parameters.

We have already seen one of the $\eta_j(t)$ transitions in Example 7 where we named it a'(t). The next example illustrates a case with non-zero $\Theta_{ij}(t)$ transitions.

Example 10: Consider a special case of the (permanent fault) reliability model of the Fault-Tolerant Multiprocessor (FTMP). Assume that there are n processors each with a constant failure rate λ. Upon occurrence of a fault there is exponentially distributed detection latency of rate δ. A fault is ultimately detected with probability 1 but if a second fault occurs while another is latent (within its detection latency phase), a coverage failure is said to have occurred. Figure 13 shows a portion of this reliability model.

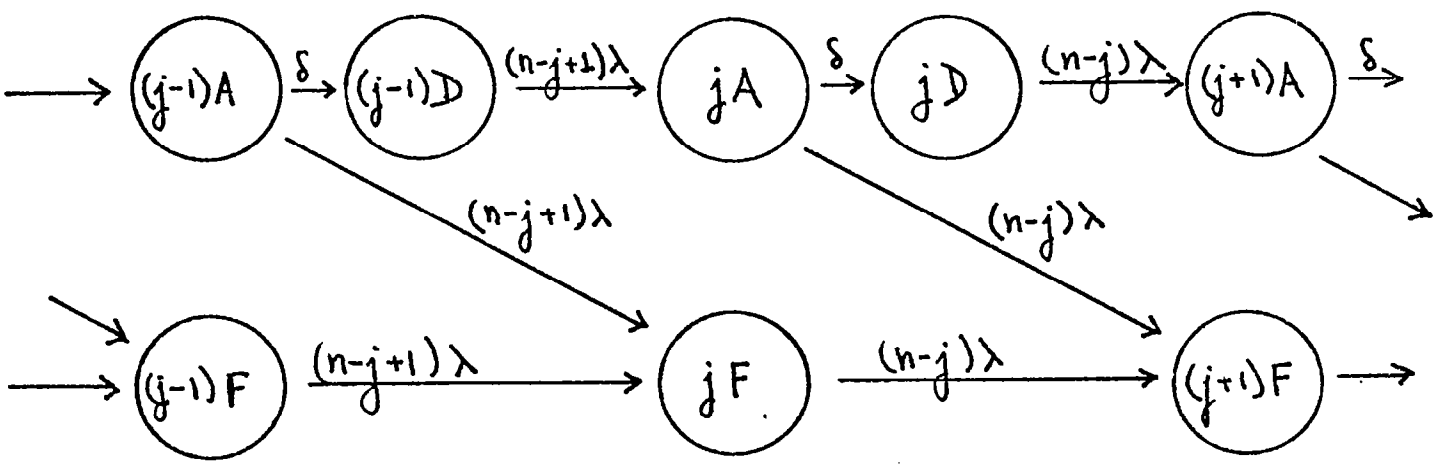

Figure 13. - Abbreviated Fault-Tolerant Multiprocessor Model.

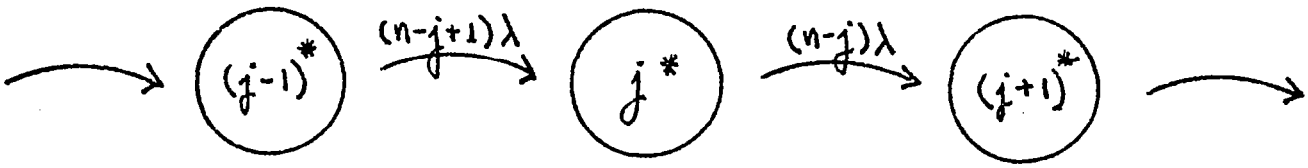

Figure 14. - Perfect Coverage Markov Chain.

First we solve for the state probabilities $P_j^*(t)$ assuming perfect coverage, using the Markov chain in Figure 14.

$$P_0^*(t) = e^{-n\lambda t} ,$$

$$P_1^*(t) = \int_0^t e^{-n\lambda x} \cdot n\lambda \cdot e^{-(n-1)\lambda(t-x)}\, dx$$

$$= e^{-(n-1)\lambda t}\, n\, (1-e^{-\lambda t})$$

$$P_2^*(t) = \int_0^t P_1^*(x) \cdot (n-1)\lambda\, e^{-(n-2)\lambda(t-x)}\, dx$$

$$= \binom{n}{2} e^{-(n-2)\lambda t} (1-e^{-\lambda t})^2$$

and, in general,

$$(18) \quad P_j^*(t) = \binom{n}{j} e^{-(n-j)\lambda t} (1-e^{-\lambda t})^j , \quad j = 0,1,\ldots n .$$

Next consider the reduced version of Figure 13 shown in Figure 15. If we wish to compute $Q_j(t)$ using Formula (17), then we first need to derive an expression for $\Theta_{j-1,j}(t)$. Now it is easy to see that

$$(19) \quad \Theta_{j-1,j}(t) = \frac{(n-j+1)\lambda\, P_{(j-1)\ A}(t)}{P_{(j-1)\ A}(t) + P_{(j-1)\ D}(t)} = (n-j+1)\lambda\, y .$$

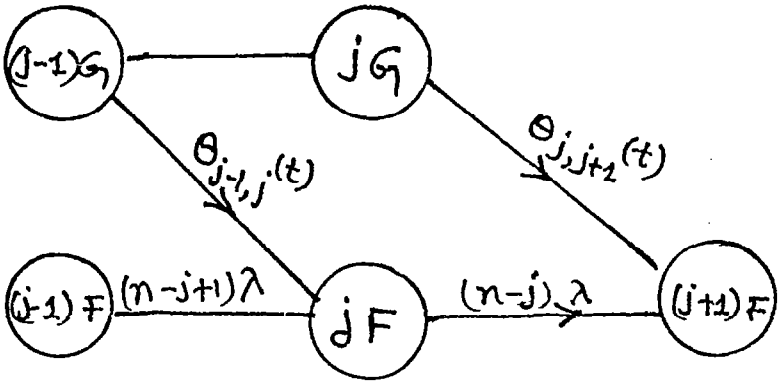

Figure 15. - Reduced Version of Figure 13.

In order to apply this formula, we need to obtain the state probabilities $P_{(j-1)\ A}(t)$ and $P_{(j-1)\ D}(t)$ for the chain of Figure 13, but this is precisely what we wanted to avoid!

We note, however, that we do not need the actual values of these probabilities but merely the ratio

$$y = \frac{P_{(j-1)\ A}(t)}{P_{(j-1)\ A}(t) + P_{(j-1)\ D}(t)} .$$

Note further that y is the conditional probability that there is a latent fault given that the system has experienced (j-1) faults.

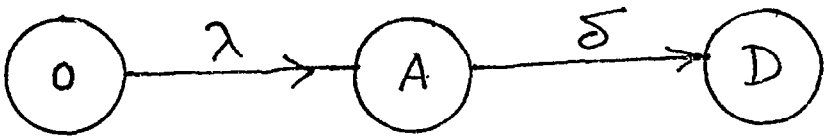

Figure 16. - Example Markov Chain with Coverage.

We claim that a good approximation to this probability can be obtained from a very simple 3-state coverage model for the specific module which has experienced the fault that forced the

system into state (j-1) A. Consider the Markov chain of Figure 16. We claim that if we compute the state probabilities for this chain, then the ratio

$$\hat{y} = (j-1)\frac{P(\text{ state A at time t})}{P(\text{state A at time t}) + P(\text{ state D at time t})},$$

is approximately equal to the ratio y that we seek! The factor (j-1) here represents the number of ways in which we could find 1 latent fault among the j-1 faults present in the system, that is, $\binom{j-1}{1}$. In a more general setting we would need the number of ways μ latent faults can be found in the system given that it has experienced j faults, that is, $\binom{j}{\mu}$ as the multiplying factor.

We now proceed with the computation:

P(state A at time t)

$$= \int_0^t P_A(t-x) * P(\text{ cov. model entered during } (x, x + dx))$$

$$= \int_0^t e^{-\lambda x} \lambda\, e^{-\delta(t-x)}\, dx$$

$$= \frac{\lambda}{\delta-\lambda}\left[e^{-\lambda t} - e^{-\delta t}\right], \text{ and similarly}$$

$$P(\text{state D at time t}) = \int_0^t P_A(x)\, \delta dx$$

$$= \frac{\lambda\delta}{\delta-\lambda}\int_0^t \left[e^{-(\lambda)x} - e^{-\delta x} \right] dx$$

$$= \frac{\lambda\delta}{\delta-\lambda}\left[\frac{1-e^{-\lambda t}}{\lambda} - \frac{1-e^{-\delta t}}{\delta}\right]$$

$$= 1 - \frac{\delta}{\delta-\lambda} e^{-\lambda t} + \frac{\lambda}{\delta-\lambda} e^{-\delta t}.$$

Hence, the required ratio is

$$\hat{y} = (j-1)\,\frac{\lambda}{\delta-\lambda}\,\frac{e^{-\lambda t} - e^{-\delta t}}{1-e^{-\lambda t}}$$

which implies that

$$(20)\quad \hat{\theta}_{j-1,j}(t) = (n-j+1)\lambda\,(j-1)\,\frac{\lambda}{\delta-\lambda}\,\frac{e^{-\lambda t}-e^{-\delta t}}{1-e^{-\lambda t}}\,.$$

The reader is urged to check that computation of $\theta_{12}(t)$ based on Formula (19) gives exactly the same answer as (20) whereas the exact computation of $\theta_{23}(t)$ gives a somewhat different answer from that produced by (20). However, for small enough values of λ/δ, the two answers tend to be rather close; for example, if we take $\lambda = 10^{-5}$ failures/hour and detection rate $\delta = 10^{2}$ $(\lambda/\delta = 10^{-7})$ we find that the two values, $\theta_{23}(t)$ and $\hat{\theta}_{23}(t)$, agree to six decimal places, for any time $t > 0$.

Now applying Formula (20), we have

$$Q_j(t) \equiv \int_0^t Q_{j-1}(x)\;(n-j+1)\lambda\; e^{-(n-j)\lambda(t-x)}\;dx$$

$$+\int_0^t P^*_{j-1}(x)\;(n-j+1)\lambda\;\frac{\lambda(j-1)}{\delta-\lambda}\;\left(\frac{e^{-\lambda x}-e^{-\delta x}}{1-e^{-\lambda x}}\right)\;e^{-(n-j)\lambda(t-x)}\;dx.$$

where $Q_0(t) = 0$,and $P^*_j(t)$ is given in (18).

Then using (18), we have

$$Q_j(t) = (n-j+1)\lambda\, e^{-(n-j)\lambda t}\left[\int_0^t Q_{j-1}(x)\, e^{(n-j)\lambda x} dx\right.$$

$$\left.+\int_0^t \binom{n}{j-1} e^{-(n-j+1)\lambda x} \frac{(1-e^{-\lambda x})^{j-1}}{(1-e^{-\lambda x})} (j-1)\, \frac{\lambda}{\delta-\lambda}\left(e^{-\lambda x}-e^{-\delta x}\right) e^{(n-j)\lambda x} dx\right]$$

$$= (n-j+1)\lambda\, e^{-(n-j)\lambda t}\left[\int_0^t Q_{j-1}(x)\, e^{(n-j)\lambda x}\, dx\right.$$

$$\left.+\int_0^t \binom{n-2}{j} n(n-1)\left[e^{-2\lambda x}-e^{-(\delta+\lambda)x}\right](1-e^{-\lambda x})^{j-2}\right] .$$

#

Example 11: We can observe another transition of the η_j type when we consider the 2-unit system of Figure 17, which incorporates

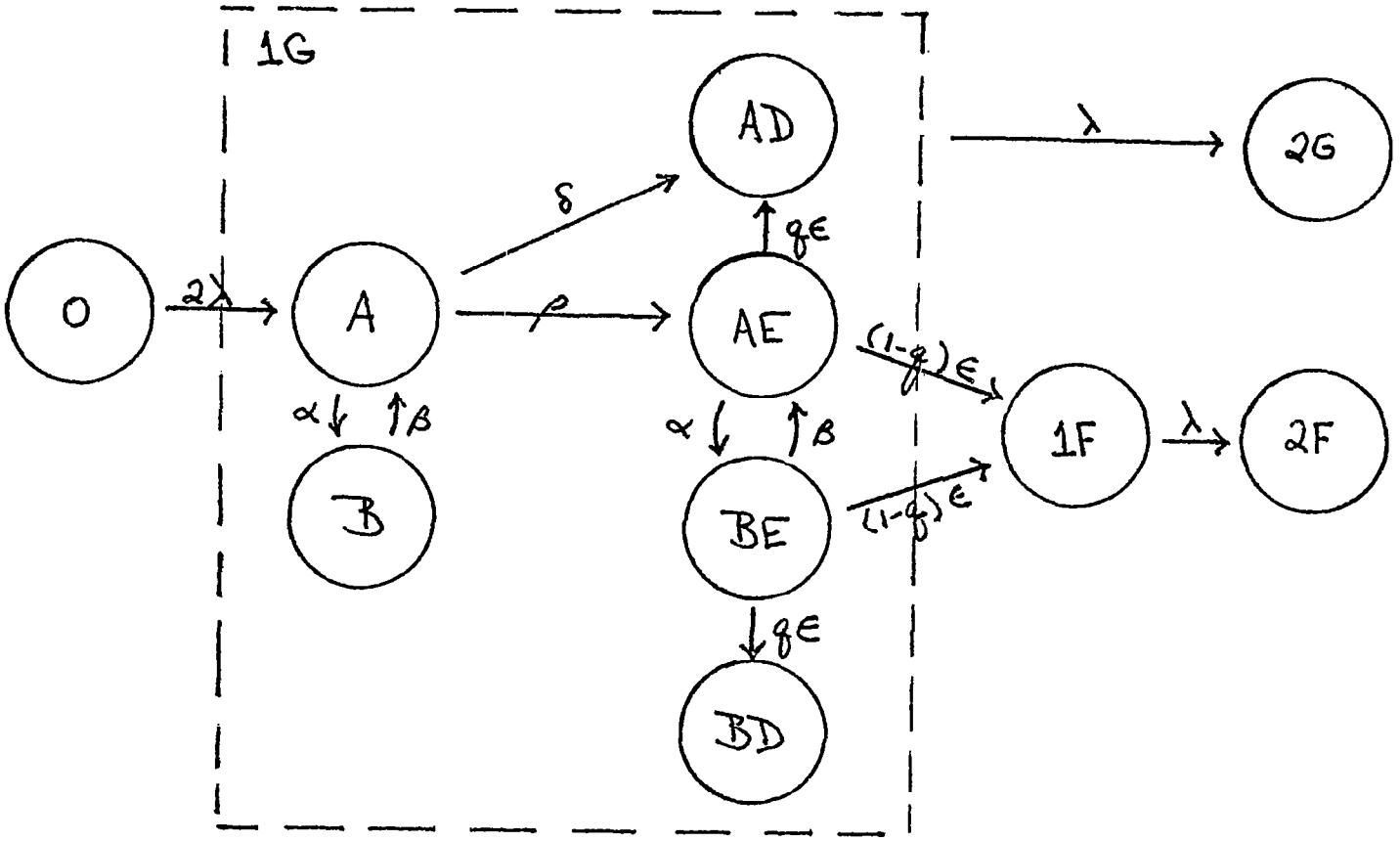

Figure 17. - Two Unit System Model with Full CARE III Single Fault Coverage Model.

the full CARE III single fault coverage model. Errors are generated at rate ρ only from the active state, but, once generated, can propagate from either active or benign states.

The corresponding perfect coverage model was given in Example 2, and, if $\alpha = \beta = 0$, we are here carrying out the analysis begun in Example 8.

To avoid the unpleasantness of recursive formulas, we consider the case $\beta = 0$ (though α need not be 0). Now clearly

$$\eta_1(t) = \frac{(1-q)*[P(\text{state AE at time } t)*P(\text{state BE at time } t)]}{P(\text{state A or B or AE or BE or AD or BD at time } t)}$$

$$= \frac{(1-q)\epsilon \int_0^t [p_{AE}(t-x)+p_{BE}(t-x)]\lambda e^{-\lambda x}\, dx}{\int_0^t (1-p_{1F}(t-x))\ \lambda e^{-\lambda x} dx}$$

where again $p_j(t-x) = P(\text{coverage model state } j \text{ at time } t, \text{ given entry at time } x)$. Using convolutions, we have

$$p_{AE}(\tau) = \int_0^\tau e^{-(\rho+\alpha+\delta)(\tau-y)} \rho\ e^{-(\epsilon+\alpha)y}\, dy$$

$$= \frac{\rho}{\rho+\delta-\epsilon} \left[e^{-(\alpha+\epsilon)\tau} - e^{-(\alpha+\rho+\delta)\tau}\right]$$

$$p_{BE}(\tau) = \int_0^\tau p_{AE}(\tau-y)\ \alpha\ e^{-\epsilon y}\, dy$$

$$= \frac{\rho}{\rho+\delta-\epsilon} \left[(e^{-\epsilon\tau} - e^{-(\alpha+\epsilon)\tau}) - \left(\frac{\alpha(e^{-\epsilon\tau} - e^{-(\alpha+\rho+\delta)\tau})}{\alpha+\rho+\delta-\epsilon}\right)\right]$$

so that

$$p_{AE}(t-x)+p_{BE}(t-x) = \frac{\rho}{\alpha+\rho+\delta-\epsilon} \left[e^{-\epsilon(t-x)} - e^{-(\alpha+\rho+\delta)(t-x)}\right].$$

Further,

$$p_{1F}(t) = \int_0^{\tau} (1-q)\epsilon [\, p_{AE}(y) + p_{BE}(y) \,]\, dy$$

$$= \frac{(1-q)\rho}{\alpha+\rho+\delta} - \frac{(1-q)\rho}{\alpha+\rho+\delta-\epsilon} e^{-\epsilon\tau} + \frac{(1-q)\epsilon\rho}{(\alpha+\rho+\delta-\epsilon)(\alpha+\rho+\delta)} e^{-(\alpha+\rho+\delta)\tau}$$

so

#

$$\eta_1(t) =$$

$$\frac{(1-q)\epsilon\rho\lambda e^{-\lambda t}}{(\lambda-\epsilon)(\lambda-(\alpha+\delta+\rho))} + \frac{(1-q)\epsilon\rho\lambda e^{-\epsilon t}}{(\alpha+\rho+\delta-\epsilon)(\lambda-\epsilon)} - \frac{(1-q)\epsilon\rho\lambda e^{-(\alpha+\rho+\delta)t}}{(\alpha+\rho+\delta-\epsilon)(\lambda-(\alpha+\rho+\delta))}$$

$$\frac{\alpha+\delta+\rho q}{\alpha+\rho+\delta} - \left[1 - \frac{\rho\epsilon(1-q)}{(\lambda-\epsilon)(\lambda-(\alpha+\rho+\delta))}\right] e^{-\lambda t} + \left[\frac{\lambda\rho(1-q)e^{-\epsilon t}}{(\alpha+\rho+\delta-\epsilon)(\lambda-\epsilon)}\right] + \left[\frac{\lambda\epsilon\rho(q-1)e^{-(\alpha+\rho+\delta)t}}{(\alpha+\rho+\delta)(\alpha+\rho+\delta-\epsilon)(\lambda-(\alpha+\rho+\delta))}\right]$$

Now $Q_0(t) = 0$, and $Q_1(t)$ may be approximated by

$$Q_1(t) = \int_0^t P_1^*(x)\ \eta_1(x)\ e^{-\int_x^t \lambda_1(\tau)\, d\tau}\ dx$$

$$= 2\, e^{-\lambda t} \int_0^t (1-e^{-\lambda x})\ \eta_1(x)\ dx$$

Since the rate λ is, in practice, several orders of magnitude smaller than any rate $\gamma \in \{\alpha, \delta, \rho, \epsilon\}$, it is reasonable to consider $Q_1(t)$ as $\frac{\lambda}{\gamma} \to 0$; in this case the integral simplifies considerably:

$$Q_1(t) \cong \frac{(1-q)\rho}{\alpha+\delta+\rho q} 2(e^{-\lambda t} - e^{-2\lambda t}).$$

This same consideration (λ / γ-->0) can be used here to gain an estimate of the error introduced by using $P_j^*(t)$ rather than $P_j(t)$ in computing $Q_j(t)$. If we write $\eta_1(t) = N(t) / D(t)$, then by solving the complete Markov model of this example (with no separation of coverage) we find

$$P_1(t) = 2\ e^{-\lambda t}\ D(t)$$

so that $\eta_1(t) = 2\ e^{-\lambda t}\ N(t) / P_1(t)$, thus giving us a fortuitous cancellation in

$$Q_1(t) = \int_0^t P_1(x)\ \eta_1(x)\ e^{-\lambda(t-x)}\ dx\ .$$

If λ/γ--> 0 now we obtain

$$Q_1(t) = \frac{(1-q)\ \rho}{\alpha+\delta+\rho}\ 2\ (e^{-\lambda t} - e^{-2\lambda t})$$

which can easily be compared with the earlier approximate value to show the extent of the under-estimation of system reliability introduced by using P_1^*. Note that unless $\left| \frac{Q_1(t)-\hat{Q}_1(t)}{Q_1(t)} \right|$ is small compared to 1 (equivalently, $\frac{(1-q)\ \rho}{\alpha+\delta+\rho\ q}$ is small compared to 1), the error is substantial.

#

Example 12: Transitions of all four types (λ_{ij}, θ_{ij}, γ_{ij} and η_j) can be illustrated in the 3-unit model of Figure 18, which incorporates the CARE III double-fault coverage model, as well as two CARE III single-fault models.

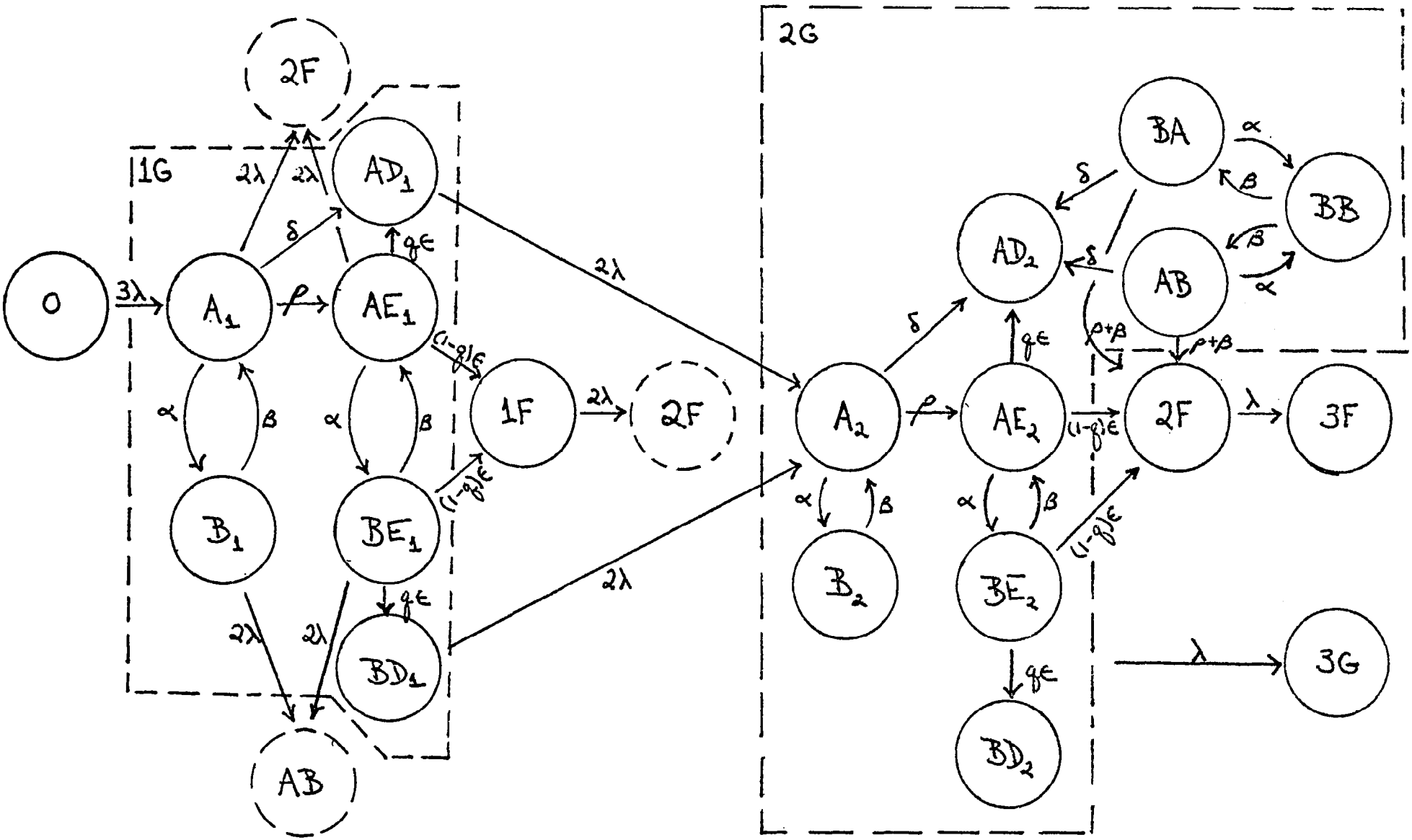

Figure 18. - Three Unit System Model with CARE III Double Fault Coverage Model and Single Fault Models.

The occurrence of a second fault while the first is in an active state (A_1 or AE_1) causes immediate system failure, thus a θ_{12} type transition. Should the first fault be in a benign state, the second forces entry into the double fault model, from which we have detection or system failure, the latter due to either both faults becoming active or a single active fault generating an error. Thus system failures from the double fault model are of the η_2 type, as are uncovered propagated errors from the states AE_2 and BE_2. Of course, we still have η_1 type transitions from states AE_1 and BE_1 as well as the obvious γ_{ij} and λ_{ij} types present in Example 11. The corresponding perfect coverage model of Figure 19 is easily seen to have solution

$$P_0^*(t) = e^{-3\lambda t},$$

$$P_1^*(t) = 3(e^{-2\lambda t} - e^{-3\lambda t}),$$

$$P_2^*(t) = 3(e^{-\lambda t} - 2 e^{-2\lambda t} + e^{-3\lambda t}), \text{ and}$$

$$P_3^*(t) = 1 - e^{-3\lambda t} + 3 e^{-2\lambda t} - 3 e^{-\lambda t}.$$

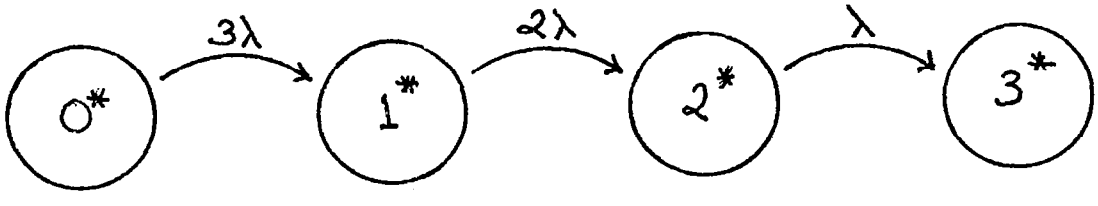

Figure 19. - Perfect Coverage Model for Figure 18 System.

Again $Q_0(t) = 0$, and

$$Q_1(t) \cong \int_0^t P_1^*(x)\eta_1(x)\, e^{-\int_x^t \lambda_1(\tau)d\tau}\, dx$$

where η_1 is computed using a single-fault coverage model identical to that in Example 11, and $\lambda_1(\tau) = 2\lambda$. Thus

$$Q_1(t) \cong 3e^{-2\lambda t}\int_0^t (1-e^{-\lambda x})\ \eta_1(x)\ dx.$$

If we again consider $\frac{\lambda}{\gamma}$-->0, then, using the computation of this integral already carried out in Example 11, we have

$$Q_1(t) \cong \frac{3(1-q)\rho}{\alpha+\delta+\rho\ q}\ (e^{-2\lambda t}-e^{-3\lambda t})\ .$$

Here, again, if we use P_1 rather than P_1^* we obtain

$$Q_1(t) = \frac{3(1-q)\ \rho}{\alpha+\delta+\rho}\ (e^{-2\lambda t}-e^{-3\lambda t}\ )\ .$$

$$\text{Now } Q_2(t) = \int_0^t Q_1(x)\lambda_{12}(x)\, e^{-\int_x^t \lambda_2(\tau)\ d\tau}\, dx$$

$$+ \int_0^t P_1(x)\ \theta_{12}(x)\, e^{-\int_x^t \lambda_2(\tau)d\tau}\, dx$$

$$+ \int_0^t P_2(x)\ \eta_2(x)\, e^{-\int_x^t \lambda_2(\tau)\ d\tau}\, dx\ .$$

Clearly, $\lambda_{12} = 2\lambda$, $\lambda_2 = \lambda$, and

$$\theta_{12}(t) = \frac{2\lambda\ [P(\text{state } A_1 \text{ at time } t) + P(\text{state } AE_1 \text{ at time } t)\ ]}{P_1(t)},$$

which is again easily computed as in Example 11, using the

single-fault model in isolation. Finally, as mentioned earlier, η_2 has two components, one from the double-fault model:

$$\frac{(\rho+\beta)\ [P(\text{state AB})+P(\text{state BA})\ ]}{P_2(t)}$$

and one from the second single-fault model:

$$\frac{(1-q)\epsilon\ [P(\text{state } AE_2)+P(\text{state } BE_2)\ ]}{P_2(t)}$$

Note, however, that this "second single-fault model" is actually an integral part of the "double-fault model", and it is this joint coverage model which must be considered when calculating these last ratios in the style of Example 11.

If we again restrict ourselves to $\beta = 0$ and consider $\frac{\lambda}{\gamma} \dashrightarrow 0$, then we obtain

$$Q_2(t)=\frac{\rho\alpha\ q+2(\alpha+\delta)\ \rho(1-q)+\rho^2(1-q^2)}{(\alpha+\delta+\rho)^2}\ 3[e^{-\lambda t}-2e^{-2\lambda t}+e^{-3\lambda t}\ ]\ .$$

#

4.3 Coverage Model Calculations

In this section, we consider general methods of deriving the transition parameters $\eta_j(t)$ and $\Theta_{ij}(t)$. It should be noted from our previous examples that since we only compute $Q_j(t)$ and $P_j^*(t)$, we never need the parameters $\gamma_{ij}(t)$.

First we consider the parameter $\eta_j(t)$. This parameter arises from those latent faults that give rise to a coverage failure in absence of any additional faults. It is certainly possible, in general, for a single latent fault by itself to give rise to a coverage failure. This situation will be captured by a general single fault model that we will discuss. It is also possible for a combination of interacting (non-independent) latent faults to give rise to a coverage failure. To capture such a situation, we have to consider all possible system states due to such an interacting set of latent faults. In order to avoid such complexity, we only consider all pairs of interacting latent faults (in a general double-fault model) and assume that a third (interacting) fault will immediately give rise to a coverage failure.

Unlike all the examples we have considered earlier, the two coverage models we consider here are semi-Markov processes. The main references on this topic are [23, 24]. A semi-Markov process shares with a Markov process the property that state transitions are regeneration points obliterating the influence of the past. However, the holding time in a state is no longer assumed to be exponentially distributed. Thus we will model the time dependency of transition parameters where the (local) time is measured from the entry into the specific state. This is in contrast to the non-homogeneous Markov chain where the time-dependency of transition parameters with respect to global time only was allowed.

Consider a general semi-Markov process shown in Figure 20. Events that cause a transition from state i to state j occur at the

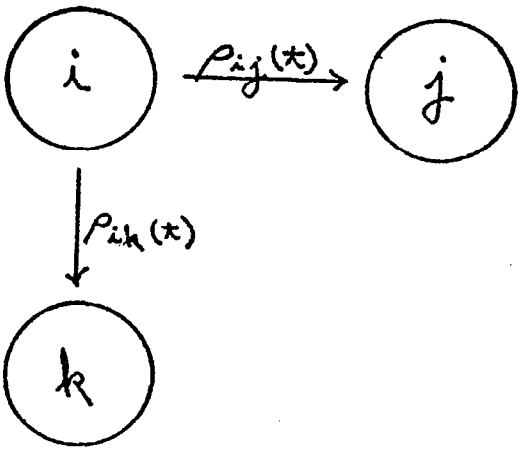

Figure 20. - General Semi-Markov Process

rate $h_{ij}(t)$, independently of the events causing other transitions. Let

$$\rho_{ij}(t) = h_{ij}(t)\ r_{ij}(t) \text{ where}$$

$$r_{ij}(t) = e^{-\int_0^t h_{ij}(\tau)d\,\tau}.$$

Unlike the Markov case, we prefer to label the arcs by the corresponding pdf's ($\rho_{ij}(t)$) rather than by transition rates. Thus in this notation, an arc labelled α in a Markov chain will now be labelled $\alpha\, e^{-\alpha t}$. Let $F_{ij}(t)$ be the (unconditional) probability that a transition from state i to state j occurs in (local) time with duration $\leq t$. Then

$$F_{ij}(t) = \int_0^t \rho_{ij}(\tau) \prod_{k\neq j} r_{ik}(\tau)\ d\,\tau$$

where $r_{ik}(t) = 1-\int_0^t \rho_{ik}(\tau)\ d\,\tau$.

Let $f_{ij}(t)$ be the derivative of $F_{ij}(t)$. Note that $r_{ik}(t)$ is the

conditional probability that no transition be made to state k by time t. The holding time distribution in state i is then given by

$$F_i(t) = \sum_j F_{ij}(t) \ .$$

Feller [23] shows that

$$(21)\quad p_{ik}(t) = \delta_{ik}(1-F_i(t)) + \sum_j \int_0^t f_{ij}(x)p_{jk}(t-x)\ dx$$

where δ_{ik} is the Kronecker delta function. It should be noted that in the Markovian cases we used the forward Equation (1) all along. In the semi-Markov case the forward equation is much harder than the backward equation above.

Example 13: Consider the single-fault model shown in Figure 21. Applying Equation (21) to the present problem and remembering that state 0 is the initial state, we get

#

$$p_{AA}(t) = d(t)\ r(t)\ a(t) + \int_0^t \alpha e^{-\alpha x}\ d(x)r(x)\ p_{BA}(t-x)\ dx$$

$$p_{BA}(t) = \int_0^t \beta\ e^{-\beta x} p_{AA}(t-x)\ dx$$

$$p_{AA}(t) = d(t)\ r(t)a(t) + \beta \int_0^t \alpha e^{-\alpha x}\ d(x)r(x) \int_0^{t-x} e^{-\beta\tau} p_{AA}(t-\tau-x)d\tau\ dx$$

$$= e^{-\alpha t}\ d(t)r(t) + \beta \int_0^t [\alpha e^{-\alpha x} d(x)r(x) \int_0^{t-x} e^{-\beta(t-x-y)} p_{AA}(y)dy\ dx]$$

$$= e^{-\alpha t}\ d(t)r(t) + \beta \int_0^t \int_0^{t-y} \alpha e^{-\alpha x}\ d(x)r(x)e^{-\beta(t-x-y)} p_{AA}(y)dx\ dy.$$

Let $\phi(t-y) = \int_0^{t-y} \alpha\ e^{-\alpha x} d(x)\ r(x)e^{-\beta(t-x-y)}\ dx$

and where

$$d(t) = 1 - \int_0^t \delta(\tau)\, d\tau \ ,$$

$$a(t) = 1 - \int_0^t \alpha e^{-\alpha\tau}\, d\tau = e^{-\alpha t} \ ,$$

$$r(t) = 1 - \int_0^t \alpha(\tau)\, d\tau$$

Hence

$$P_{AA}(t) = e^{-\alpha t}\, d(t)\, r(t) + \beta \int_0^t \phi(t-y)\, P_{AA}(y)\, dy.$$

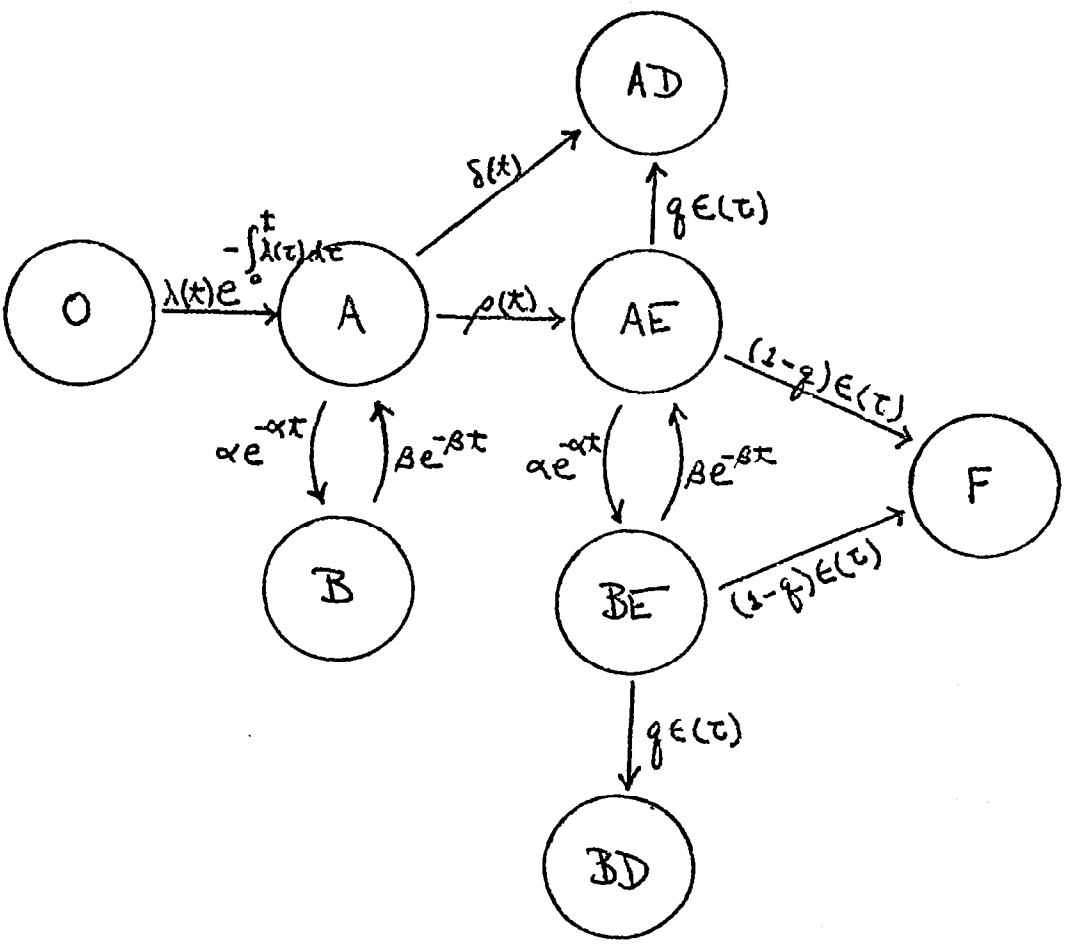

Figure 21. - CARE III Single-Fault Model

Similarly, we have,

$$p_{AB}(t) = \phi(t) + \beta \int_0^t \phi(t-y) p_{AB}(y)\, dy \ .$$

Once these probabilities are computed, we can compute

$$P_A(t) = \int_0^t \lambda(x)\, e^{-\int_0^x \lambda(\tau)\, d\tau}\, p_{AA}(t-x)\, dx$$

$$P_B(t) = \int_0^t \lambda(x)\, e^{-\int_0^x \lambda(\tau)\, d\tau}\, p_{AB}(t-x)\, dx \ .$$

Finally, the contribution to $\eta_j(t)$ by the single fault model, denoted by $a'(t)$ is given by:

$$\frac{P'_F(t)}{P_A(t) + P_B(t) + P_{A_D}(t) + P_{B_D}(t) + P_{A_E}(t) + P_{B_E}(t)}$$

#

A similar development can be given for the double fault model, however, we omit the details here.

5. Convolution Approximations

Numerous computations of convolution integrals of the form $\int_0^t f(t-\tau)\, g(\tau)\, d\tau$ are required in CARE III reliability estimation. Since one of the functions, say g, is typically from a coverage model, while the other, f, is from the fault model, one can exploit the fact that f will vary slowly (relative to g over the interval of interest) to obtain an easily-computed approximation to the convolution integral. Specifically, $f(t-\tau)$ can be replaced by the quadratic interpolation polynomial in τ which passes through points

(0,f(t)) , (t/2 ,f(t/2)), and (t,f(0)). Writing this polynomial as $a(t)+b(t)\ \tau+c(t)\ \tau^2$, one obtains

$$\int_0^t f(t-\tau)g(\tau)d\ \tau \cong a(t) \int_0^t g(\tau)d\tau+b(t) \int_0^t \tau g(\tau)d\ \tau+c(t) \int_0^t \tau^2 g(\tau)d\tau\ .$$

As an example, consider again the computation of η_1 in Example 11 of section 4.2 (this is $a'(t|\underline{1})$ in CARE III notation). In the first formulation of the CARE III model we see

$$a'(t|\underline{1}) = \frac{\int_0^t p'_F(t-\tau)r(\tau)\ \lambda(\tau)d\ \tau}{1 - r(t)}$$

where $p'_F(t-\tau) = (1-q)\in (p_{AE}(t-\tau) + p_{BE}(t-\tau)\ )$, $r(\tau) = e^{-\lambda\tau}$, and $\lambda(\tau) = \lambda$. In the later formulation we see

$$a'(t|\underline{1}) = \frac{h_F(t)}{1-r(t)}$$

where $h_F(t)$ is defined as $a_F(t)\ m_F^0(t) + b_F(t)\ m'_F(t) + c_F(t)m_F^2(t)$.

But of course

$$\int_0^t p'_F(t-\tau)\ r(\tau)\ \lambda(\tau)\ d\ \tau$$

$$= \int_0^t p'_F(\tau)\ r(t-\tau)\ \lambda(t-\tau)\ d\ \tau, \text{ so}$$

$r(t-\tau)\ \lambda(t-\tau)$ is the fault model function f, p'_F is the coverage model function g, and

$$m_F^i(t) = \int_0^t \tau^i\ p'_F(\tau)\ d\ \tau\ .$$

Finally, the careful reader has perhaps noticed a difference in denominator between the expressions for $a'(t|\underline{1})$ above and those given in Example 11 of section 4. This difference is introduced to compensate for the $P_1 \text{-->} P_1^*$ substitution: again, if we write $\eta = a' = N/D$, then

$$P_1 \eta = P_1(2 e^{-\lambda t} N / 2e^{-\lambda t} D) = P_1(2e^{-\lambda t} N / P_1) = 2e^{-\lambda t} N .$$

If we plan to substitute P_1^* for P_1 in $P_1(N / D)$, then an exact compensation occurs if we also substitute $P_1^* / 2e^{-\lambda t}$ for D; but $P_1^* / 2e^{-\lambda t} = 1-e^{-\lambda t} = 1-r(t)$, as above.

6.0 Concluding Remarks

CARE III is an advanced reliability prediction tool developed by Raytheon under the sponsorship of NASA Langley Research Center. Because of sophisticated mathematics employed by CARE III, it was deemed desirable to provide an independent view and a tutorial of various important concepts employed. As of this writing, details of CARE III are evolving, and therefore, no attempt has been made to track its developments in complete detail. Most of the concepts outlined here remain valid in spite of the later changes to CARE III.

Major notions used in CARE III are that of behavioral decomposition followed by aggregation in an attempt to deal with reliability models with a large number of states. A comprehensive set of models of the fault-handling processes in a typical fault-tolerant system have been used. These models are semi-Markov in nature, thus removing the usual restrictions of exponential holding times within the coverage model. The aggregate model is a non-homogeneous Markov

chain, thus allowing the times to failure to possess Weibull-like distributions. Because of the departures from traditional models, the solution method employed is that of Kolmogorov integral equations, which are evaluated numerically.

There are several sources of errors in the CARE III model. First, the decomposition/aggregation process involves the error in estimating the transition parameters such as $\theta_{j-1,j}(t)$ on the basis of the analysis of a single module rather than the entire system. Second, the substitution of $P_j^*(t)$ in place of $P_j(t)$ in solving for $\theta_j(t)$ introduces errors. Similarly, the θ_j states are treated as terminal states in the actual CARE III model (refer to Examples 2 and 3) which introduces errors. It is recommended that a theoretical analysis of these errors be carried out and bounds on these errors be obtained. Experimental analysis of these errors is also desirable.

Yet another source of errors is numerical in nature. The numerical integration carried out to obtain $\theta_j(t)$ involves discretization and round-off errors. The convolution integration in solving for coverage models contains truncation errors. These errors also need to be analyzed.

7.0 References

1. Trivedi, K.S., J.W. Gault, and J.B. Clary, "The Validation of System Reliability in Life-Critical Applications," Proceedings, Pathways to System Integrity Symposium, National Bureau of Standards, Gaithersburg, MD, June 19, 1980.

2. Gault, J.W., K.S. Trivedi, and J.B. Clary, eds., "Validation Methods Research for Fault-Tolerant Avionics and Control Systems - Working Group Meeting II." NASA CP-2167, 1980.

3. Mathur, F.P. and A. Avizienis, "Reliability Analysis and Architecture of a Hybrid-Redundant Digital System: Generalized Triple Modular Redundancy with Repair," Proc. AFIPS SJCC, 1970.

4. Bouricius, W.G., W.C. Carter, and P.R. Schneider, "Reliability Modeling Techniques for Self-Repairing Computer Systems," Proc. 24th National Conference of ACM, 1969, pp. 295-383.

5. Stiffler, J.J., et al., "An Engineering Treatise of the CARE II Dual Mode and Coverage Models," Final Report, NASA CR-144993, April 1976.

6. Ng, Y.W. and A. Avizienis, "A Model for Transient and Permanent Fault Recovery in Closed Fault-Tolerant Systems," Proc. 1976 Int. Symposium on Fault-Tolerant Computing, June 1976.

7. Ng, Y.W. and A. Avizienis, "ARIES - An Automated Reliability Estimation System," Proc. 1977 Annual Reliability and Maintainability Symposium, January 1977.

8. Wensley, J., et al., "SIFT: Design and Analysis of a Fault-Tolerant Computer for Aircraft Control," Proc. of the IEEE, October 1978.

9. Hopkins, A.L., et al., "FTMP - A Highly Reliable Fault-Tolerant Multiprocessor for Aircraft Control," Proc. of the IEEE, Vol. 66, No. 10, October 1978.

10. Stiffler, J.J., L.A. Bryant, and 1. Guccione, "CARE III Final Report, Phase I," NASA Contractor Report 159122, November 1979.

11. Cox, D.R., "The Use of Complex Probabilities in the Theory of Stochastic Processes," Proc. Cambridge Philosophical Society, 1955.

12. Landrault, C. and J.C. Laprie, "SURF - A Program for Modeling and Reliability Prediction for Fault-Tolerant Computing Systems," Information Technology, J. Moneta (ed.), Amsterdam: North-Holland Publishing Company, 1978.

13. Kleinrock, L., Queueing Systems, Volumes I and II, New York, NY: Wiley Interscience, 1975 and 1976.

14. Aho, A.V., J.E. Hopcroft, and J.D. Ullman, The Design and Analysis of Computer Algorithms, Addison-Wesley, Reading, MA., 1974.

15. Tripathi, S.K., "On Approximate Solution Techniques for Queueing Network Models of Computer Systems," Tech. Report CSRG-106, University of Toronto, September 1979.

16. Courtois, P.J., Decomposability: Queueing and Computer System Applications, Academic Press, New York, 1977.

17. Feller, W., An Introduction to Probability Theory and Its Applications, Vol. II, Second Edition, John Wiley & Sons, Inc., New York, 1971.

18. Chung, K.L., Markov Chains with Stationary Transition Probabilities, 2nd ed., Springer Verlag, Berlin, 1967.

19. Arnold, T.F., "The Concept of Coverage and Its Effect on the Reliability Model of a Repairable System," IEEE Trans. on Computers, Vol. C-22, pp. 251-254, March 1973.

20. Stiffler, J.J., "Robust Detection of Intermittent Faults," Proc. of the Tenth Int. Symp. on Fault-Tolerant Computing, Kyoto, Japan, October 1980, pp. 216-218.

21. Parzen, E., Stochastic Processes, Holden-Day, San Francisco, California, 1962.

22. Buck, R.C. and E.F. Buck, Introduction to Differential Equations, Houghton Mifflin Company, Boston, MA., 1976.

23. Feller, W., "On Semi-Markov Processes," Proc. National Academy of Sciences, Vol. 51, pp. 653-659, 1964.

24. Ross, S.M., Applied Probability Models with Optimization Applications, Holden-Day, San Francisco, 1970.

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
NASA CR-3488		

4. Title and Subtitle	5. Report Date
A TUTORIAL ON THE CARE III APPROACH TO RELIABILITY MODELING	December 1981
	6. Performing Organization Code
7. Author(s)	8. Performing Organization Report No.
Kishor S. Trivedi and Robert M. Geist	
9. Performing Organization Name and Address	10. Work Unit No.
Department of Computer Science Duke University Durham, NC 27706	11. Contract or Grant No. NAG1-70
12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered Contractor Report
National Aeronautics and Space Administration Washington, DC 20546	14. Sponsoring Agency Code 505-34-43-05

15. Supplementary Notes

NASA Langley CARE III Project Engineer: Salvatore J. Bavuso
Interim Report

16. Abstract

In September 1980, a critical review of the theoretical bases of CARE III was conducted at the Research Triangle Institute by a number of eminent researchers (NASA CP-2167). The participants unanimously agreed that the CARE III math model is sound and the method valid. An area where further work was recommended is the need for a more detailed exposition of the method. This paper is the outcome of that recommendation.

The authors describe the elaborate CARE III model by utilizing a number of examples which frequently use state-of-the-art math modeling techniques as the basis for their exposition.

17. Key Words (Suggested by Author(s))	18. Distribution Statement
CARE III Reliability Fault Tolerant	UNCLASSIFIED - UNLIMITED Subject Category 59

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
UNCLASSIFIED	UNCLASSIFIED	61	A04

For sale by the National Technical Information Service, Springfield, Virginia 22161

NASA-Langley, 1981